ESCOLA DE COMANDO E ESTADO MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Maj Com MARIANO OSCAR **GÓMEZ**, Exército Argentino

Procurando um modelo de resiliência cibernética baseado nas experiências da OTAN e sua possível transferência para América do Sul

Rio de Janeiro

2019

Maj Com MARIANO OSCAR **GÓMEZ**, Exército Argentino

Procurando um modelo de resiliência cibernética baseado nas experiências da OTAN e sua possível transferência para América do Sul

Trabalho de Dissertação apresentado na Escola de Comando e Estado-Maior do Exército – Instituto Meira Mattos, como requisito para a obtenção do título de Mestre em Ciências Militares com ênfase em Defesa Nacional.

Orientadora: Prof. Dra. Karina Furtado Rodrigues

Rio de Janeiro

2019

G633p Gómez, Mariano Oscar

Procurando um modelo de resiliência cibernética baseado nas experiências da OTAN e sua possível transferência para América do Sul . / Mariano Oscar Gómez . —2019.
139 f. : il. ; 30 cm.

Orientação: Karina Furtado Rodrigues
Dissertação (Mestrado em Ciências Militares)—Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2019.
Bibliografia: f. 101-114.

1. RESILÊNCIA. 2. DEFESA CIBERNÉTICA 3. OTAN 4. ESTÔNIA 5. AMÉRICA DO SUL. I. Título.

CDD 001.53019

MARIANO OSCAR GÓMEZ

PROCURANDO UM MODELO DE RESILIÊNCIA CIBERNÉTICA BASEADO NAS EXPERIÊNCIA DA OTAN E SUA POSSÍVEL TRANSFERÊNCIA NA AMÉRICA DO SUL

Dissertação apresentada ao Programa de Pós-Graduação em Ciências Militares da Escola de Comando e Estado-Maior do Exército, como, pré-requisito para a obtenção do grau de Mestre em Ciências Militares.

Aprovada em 26 de agosto de 2019.

BANCA EXAMINADORA

KARINA FURTADO RODRIGUES – Profª Drª – Presidente
Escola de Comando e Estado-Maior do Exército

LUIZ ROGÉRIO FRANCO GOLDONI – Prof Dr – Membro
Escola de Comando e Estado-Maior do Exército

ALEJANDRO CÉSAR CORLETTI ESTRADA – Prof Dr – Membro
Universidad Alfonso X Elsabio - Madrid

Ciente: _____
MARIANO OSCAR GÓMEZ – Postulante
Escola de Comando e Estado-Maior do Exército

À minha esposa Guadalupe e meus filhos María Lucía e Santiago. Uma sincera homenagem pelo carinho e compreensão demonstrados durante a realização deste trabalho.

AGRADECIMENTOS

À Professora Doutora Karina Furtado Rodrigues, não só pela orientação firme e segura, como também, pelo incentivo e pela confiança evidenciada em todo momento. Sua dedicação se revestiu de capital importância para que eu pudesse realizar o trabalho com tranqüilidade e eficiência.

Ao Professor Doutor Alejandro Corletti Estrada, por ter me orientado na área da cibernética constituindo-se em um referente e exemplo de pessoa e profissional para mim.

Aos Oficiais do Exército Brasileiro da ECEME que tanto contribuíram com sua constante orientação e amizade. Particularmente aos Majores Guilherme Luchetti Cortinhas, André Luis da Costa Brandão, Alisson Alencar David, e aos Tenentes Coronéis Klaiton Alexandro Santanna Cota, Luiz Eduardo Santos Cerávolo, Glauber Juarez Sasaki Acácio, Anderson Silveira Lago e Enio Corrêa de Souza.

Aos quase 60 especialistas em cibernética dos 15 países consultados, que com absoluto desinteresse apoiaram a realização do trabalho, aportando qualidade e experiência, condições essenciais para que os resultados obtidos tenham utilidade.

Ao Instituto Meira Mattos e à Escola de Comando e Estado-Maior do Exército, por ter me permitido realizar o curso e acolhido como se fosse um oficial mais da sua Instituição.

Ao Exército Argentino pela confiança posta em mim para fazer o Curso de Comando e Estado-Maior na República Federativa do Brasil.

A Deus, pela proteção e orientação recebidas, principalmente nos momentos mais difíceis. Pela força necessária que recebi para resolver os problemas apresentados.

RESUMO

Os avanços tecnológicos e a crescente infraestrutura digital tornaram populações inteiras dependentes de sistemas interligados e complexos, chegando na atualidade à concepção de que todos os serviços modernos dependem do uso das Tecnologias da Informação e Comunicação (TIC). É assim que, com o aumento inevitável da dependência da tecnologia no nível global, a vulnerabilidade frente a ataques sobre a infraestrutura crítica, através do ciberespaço, também foi aumentada. Um exemplo disto foi o ataque cibernético de grande vulto que sofreu a Estônia em 2007 (até esse momento um dos países mais desenvolvidos em matéria digital no mundo), que gerou um impacto global, permitindo a tomada de conhecimento pela sociedade digital sobre a nova ameaça, possibilitando a criação de ferramentas e órgãos de cooperação entre os Estados para fazer frente àquela debilidade pouco conhecido na época. Surgiram assim órgãos como o *Cooperative Cyber Defence Centre of Excellence (CCDCOE*) da OTAN e diversas alianças relacionadas, que permitiram estabelecer normas, criar doutrina, elevar padrões de desempenho dos países da organização no âmbito cibernético, experimentar técnicas de emprego e difundir as lições aprendidas ao mundo todo. O presente trabalho pretende reforçar a necessidade de definir estratégias que possibilitem preservar os sistemas próprios dos países (principalmente os dados), dada a dificuldade de se impedir ataques e identificar suas fontes. Para traçar possíveis estratégias, tomar-se-á como base o conjunto de medidas implícitas e explícitas adotadas pelo CCDCOE. O termo que abrange essa estratégia é a “Resiliência Cibernética”, e constitui uma concepção de extrema relevância no contexto informacional atual, sendo que sua correta concepção permitiria que um sistema assumisse capacidades suficientes para se adaptar às ações inimigas no ciberespaço (geralmente anônimas e imprevisíveis), restaurando informações até instantes antes da referida ação, sem perder capacidades operativas significativas. Para isso, serão investigadas condições que conduzem à resiliência de sistemas cibernéticos, submetendo-as à análise de especialistas para criar um modelo ciber-resiliente, o qual será avaliado (aplicando a literatura de *transferência de*

políticas públicas) procurando sua possível implantação no âmbito da América do Sul.

Palavras-chave: Resiliência, Defesa Cibernética, OTAN, América do Sul, Estônia.

ABSTRACT

Technological advances and growing digital infrastructure have made entire populations dependent on interconnected and complex systems, now coming to the point that all modern services depend on the use of Information and Communication Technologies (ICT). With this inevitable increase in global dependence on technology, the vulnerability attacks on critical infrastructure through cyberspace has also been increased. An example of this was the large-scale cyber-attack that Estonia suffered in 2007 (until then one of the most developed digital countries in the world), which resulted in a global impact, making the digital society more aware of the new threat and enabling creation of tools and inter-state organizations to deal with that little known vulnerability at the time. Organizations such as NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) and several related alliances have resulted in establishing standards, building doctrine, raising the organization's performance standards in cybernetics, experimenting with employment techniques and disseminating lessons learned to the whole world. The present task at hand is to reinforce the need to define strategies that allow preserving a countries' own systems (mainly data), given the difficulty of preventing attacks and identifying their sources. Possible outline of strategies will be based on the implicit and explicit set of measures adopted by the CCDCOE. The term encompassing this strategy is "Cybernetic Resilience," which involves a concept of extreme relevance in the current informational context; its correct conception allows a system to assume sufficient capacities to adapt to enemy actions in cyberspace (usually anonymous and unpredictable), restoring information up to moments before said action, without losing significant operational capacities. Finally, conditions will be established that lead to the resilience of cybernetic systems, subjecting them to the analysis of specialists to create a cyber-resilient model, which will be evaluated (applying the policy transfer literature) looking for its possible implantation within South America.

Keywords: Resilience, cyber defense, NATO, South America, Estonia.

LISTA DE QUADROS E GRÁFICOS

QUADROS:

- **QUADRO 1 –** Comparação entra transferência e difusão de políticas.
- **QUADRO 2** – Quadro de síntese de resultados dos questionários dos especialistas.
- **QUADRO 3 –** Modelo preliminar de condições, subcondições e componentes necessários para que um sistema seja considerado como ciber-resiliente.
- **QUADRO 4 –** Assuntos ou condições mais relevantes tidas em conta das contribuições dos especialistas.
- **QUADRO 5 –** Categorização das opiniões dos especialistas.
- **QUADRO 6 –** Modelo final de condições, subcondições e componentes necessários para que um sistema seja considerado como ciber-resiliente.
- **QUADRO 7 –** Visão de Dolowitz e Marsh (2000) ao respeito da transferência de políticas
- **QUADRO 8 –** Síntese de revisão acadêmica de Benson e Jordan (2011).
- **QUADRO 9 –** Síntese de noticias oficiais sobre a participação da OEA na área da cibernética.
- **QUADRO 10 –** Síntese de assuntos contidos no modelo a ser transferido.
- **QUADRO 11 –** Graus de transferência para o modelo pretendido.

GRÁFICOS:

- **GRÁFICO 1 –** *FM Global Resilience Index*.
- **GRÁFICO 2 –** Evolução das Inovações Tecnológicas.
- **GRÁFICO 3 –** Brecha entre Ataque e Resposta.
- **GRÁFICO 4 –** Eficiência dos ataques cibernéticos na atualidade.
- **GRÁFICO 5 –** Mapa com o nível de compromisso em segurança cibernética.
- **GRÁFICO 6 –** Esquematização do tratamento dos dados nos capítulos segundo e terceiro

- **GRÁFICO 7 -** Representação geográfica do esforço de coleta de dados da pesquisa
- **GRÁFICO 8** – Resultados quantitativos dos questionários aos especialistas
- **GRÁFICO 9 –** Esquematização das condições causais obtidas do processo de análise de evidências.

LISTA DE ABREVIATURAS E SIGLAS

- **ARA**: Armada da República Argentina.
- **CCDCOE**: Cooperative Cyber Defense Center of Excellence.
- **CDS**: Conselho de Defesa Sul Americano.
- **CECCD**: Centro de Excelência Cooperativo de Ciber Defesa.
- **CERT**: Computer Emergency Response Team.
- **CERT-EE**: Computer Emergency Response Team for Estonia.
- **CICTE:** Comitê Interamericano contra o Terrorismo da OEA.
- **CIR**: Cyber Incident Response.
- **EA**: Exército Argentino.
- **EA-R**: Exército Argentino – Da Reserva.
- **FAA**: Força Aérea Argentina.
- **INUS**: Insufficient but necessary and unnecessary but sufficient.
- **ISA**: Information System Security.
- **OTAN**: Organização de tratados do Atlântico Norte.
- **OEA:** Organização de Estados Americanos.
- **PROSUL:** Foro para o Progresso Sul-Americano.
- **RELCOM**: Reliable Communications.
- **SUIN**: Sufficient but unnecessary and Insufficient but necessary.
- **TIC**: Tecnologia da Informação e das Comunicações.
- **UNASUL**: União de Nações Sul Americanas.

SUMÁRIO

ASSUNTO	PÁGINA
INTRODUÇÃO	**15**
1. REFEENCIAL TEÓRICO E METODOLÓGICO	**30**
1.1 **REFERENCIAL TEÓRICO**	**30**
1.2. **METODOLOGIA**	**41**
1.2.1 TRATAEMENTO DOS DADOS	**42**
1.2.2 COLETA DE DADOS	**45**
2. A OTAN E A RESILIÊNCIA CIBERNÉTICA	**47**
2.1 EVOLUÇÃO DE ESTÔNIA NO CAMPO CIBERNÉTICO ATÉ O CIBERATAQUE MASSIVO DE 2007	**47**
2.2 MEDIDAS ADOTADAS PELA ESTÔNIA E PELA OTAN APÓS OS ATAQUES CIBERNÉTICOS DE 2007	**50**
2.3 COMPONENTES ESSENCIAIS QUE PODERIAM TRANSFORMAR UM SISTEMA EM CIBER-RESILIENTE	**52**
3. PROCURANDO UM MODELO CIBER-RESILIENTE	**61**
4. É POSSÍVEL UMA AMÉRICA DO SUL CIBER-RESILIENTE?	**78**
4.1 POR QUE SE PRETENDE QUE ATORES PARTICIPEM NA TRANSFERÊNCIA DE POLÍTICAS NO ÂMBITO DA RESILIÊNCIA CIBERNÉTICA?	**86**
4.2 QUEM SÃO OS ATORES CHAVE ENVOLVIDOS NO PROCESSO DE TRANSFERÊNCIA DE POLÍTICAS ENTRE A OTAN E A AMÉRICA DO SUL?	**87**
4.3 O QUÊ SE PRETENDE TRANSFERIR E DE ONDE FORAM EXTRAIDAS AS LIÇÕES PARA SEJA FEITA?	**93**
4.4 QUAIS SÃO OS DIFERENTES GRAUS DE TRANSFERÊNCIA E QUAL SUA POSSÍVEL PROJEÇÃO NO TEMPO?	**95**
4.5 QUAIS FATORES PERMITEM E LIMITAM O PROCESSO DE POLÍTICAS NO CASO PARTICULAR DA AMÉRICA DO SUL?	**97**
CONSIDERAÇÕES FINAIS	**98**

ASSUNTO	PÁGINA
REFERÊNCIAS	**102**
APÊNDICE A – Esquema Gráfico de Pesquisa	**117**
APÊNDICE B – Processo de Elaboração de Questionário	**119**
APÉNDICE C – Questionário de Pesquisa	**121**
APÉNDICE D – Especialistas a Serem Consultados	**130**

INTRODUÇÃO

Os avanços tecnológicos e a crescente infraestrutura digital tornaram populações inteiras dependentes de sistemas interligados e complexos. A demanda por Internet e conectividade digital requer uma crescente integração das Tecnologias de Informação e Comunicação (TIC) em produtos que anteriormente funcionavam sem essas ferramentas, como nos sistemas de controle de barragens; controle de tráfego; redes nacionais de saúde; distribuição de energia, água e esgoto; gestão de transporte multimodal; tráfego aéreo; movimentações bancárias (transferências, depósitos e pagamentos) e compras *online*. Hoje, praticamente, todos os serviços modernos dependem do uso das TIC.

A chegada e consequente evolução do ciberespaço transformou o mundo e revolucionou o cotidiano dos habitantes do globo. É um ambiente que não tem fronteiras geográficas, está ao alcance de qualquer um (a tecnologia é econômica). Neste cenário os atores são anônimos, que vão desde adolescentes até organizações criminosas, alguns operando de maneira independente e outros apoiados por entes governamentais.

A partir dessa realidade, e tomando à Estônia como ponto de partida da nossa análise é que se procurará entender as variáveis que levaram a esse país a se constituir como um Estado com resiliência cibernética, avaliando-as e conformando um mecanismo que demonstre seu funcionamento.

Mesmo tendo identificadas variáveis e suas condições a grande pergunta seria: quais são as que conduzem à resiliência de um sistema cibernético? Além disso, por que foi escolhida a Estônia com referência? A primeira pergunta reveste um trabalho aprofundado para ser respondida, que será desenvolvido ao longo do documento. Ao respeito da segunda, uma resposta simples e prematura que poderia ser dada seria que o ataque cibernético sofrido pela Estônia em 2007 é reconhecido como o primeiro ataque massivo deste gênero na história. Tal evento marcou o início do que hoje é chamada de guerra cibernética (FERRERO, 2013), e levou a esse país ao grau de consciência situacional ao respeito da importância da temática que tem na atualidade.

A Estônia, para aquela época, era um dos países com menor brecha digital[1] do mundo e um dos mais evoluídos em matéria de TIC. No entanto, sua evolução tecnológica foi atingida de maneira severa no dia 26 de abril de 2007 a partir de uma série de ataques cibernéticos. Estes foram perpetrados após a decisão do governo local em derrubar o monumento ao Soldado de Bronze de Tallinn, um símbolo da influência da então União Soviética para países Bálticos.[2]

O´Connor (2003) afirma que o Soldado de Bronze é um monumento soviético da Segunda Guerra Mundial inaugurado em Tallin (Estônia) em 22 de setembro de 1947 e que tem um valor significativo tanto para os russos quanto para a população da Estônia, já que é um símbolo da ocupação soviética de 1940 até 1991, sendo que entre 1941 e 1944 a Estônia foi ocupada pela Alemanha, no contexto da Segunda Guerra Mundial, e as forças soviéticas a reconquistam ficando parte da União de Repúblicas Socialistas Soviéticas até 1991.

Segundo Aviar (2007), em abril de 2007, o governo da Estônia decidiu trasladar o Soldado de Bronze e os restos dos soldados soviéticos, depois de exumados e identificados, ao cemitério militar das Forças de Defesa da Estônia em Tallin, no meio de controvérsias políticas internas e externas ao país. Essas controvérsias, exteriorizadas a partir de manifestações, distúrbios, medidas de força e tensões diplomáticas entre os países, culminou com aquela sucessão de ataques cibernéticos sem precedentes até esse momento na história.

Czosseck, Ottis e Taliharm (2011) descrevem que o período dos ataques cibernéticos na Estônia ocorreu entre 27 de abril e 18 de maio de 2007. Eles foram realizados em duas fases: uma inicial, entre 27 e 29 de abril, caraterizada pela utilização de ferramentas, rudimentares, contra sítios *web* do Ministério da Defesa e de outras estruturas do Estado, além de partidos

---

1 Serrano [et al] (2003) define brecha digital como “a separação que existe entre as pessoas (comunidades, estados, países, etc) que utilizam as Tecnologias da Informação e Comunicações (TIC) como uma parte rotineira da sua vida diária e aquelas que não tem acesso às mesmas e que, mesmo as tenham, não sabem como utilizá-las” (p. 175, tradução nossa).

2 Ottis (2008) afirma que, para a minoria local russa, o soldado (de bronze) representa ao libertador, mesmo que para os estônicos represente o opressor.

políticos; e a outra fase, a partir de 30 de abril até 18 de maio, com ataques mais complexos e coordenados.

A partir disto, a OTAN e a União Europeia ofereceram apoio ao país, dando cumprimento ao estabelecido no Tratado de Washington (ou Tratado do Atlântico Norte), de 4 de abril de 1949.

Ferrero (2013) afirma que “o ciberataque à Estônia em 2007 [...] representa a primeira ocasião em que um Estado-membro solicita apoio à OTAN por um ataque à infraestrutura crítica de informação do país” (p.93, tradução nossa).

Ao término das operações cibernéticas na Estônia, começaram se desenvolver ideias e medidas de cooperação cibernéticas de fato, conforme o exposto por McNamara (2010). Prova disto é a criação do Centro de Coordenação de Defesa Cibernética, chamado de “Defesa do Tigre”, tendo como base a Estônia, principal interessada no assunto.

Assim, em 14 de Maio de 2008, foi criado o CCDCOE (*Cooperative Cyber Defense Centre of Excellence*), contando inicialmente com os seguintes países: Alemanha, Eslováquia, Espanha, Estônia, Itália, Letônia e Lituânia os países participantes. Com a adesão de muitos países, apenas cinco meses depois, a iniciativa alcançou o status de Organização Militar Internacional (TADDEO; GIORIOSO, 2017). Em 2010 incorporou-se a Hungria, em 2011 os Estados Unidos da América e a Polônia, em 2012 a Holanda e em 2014 a França, o Reino Unido, a República Checa e a Áustria (este não membro da OTAN).

Estrada (2017) deixa em evidência que o ataque cibernético recebido pela Estônia teve impacto mundial, conscientizando a sociedade digital sobre a ameaça e a necessidade dos países em cooperarem e se tornarem proativos ante a questão cibernética. Baseados nesse contexto, é que começam a surgir conceitos como a Resiliência, que abrange diversas áreas disciplinares, sendo sua origem a Física.

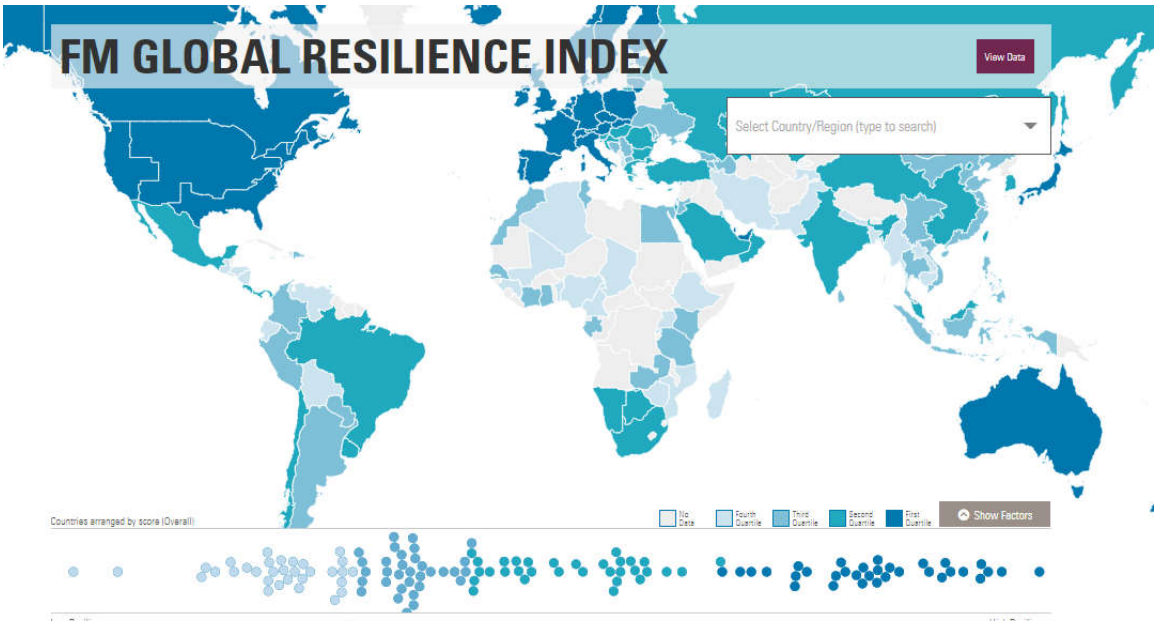
Dessa maneira, o termo Resiliência poderia ser incorporado ao ambiente cibernético com adaptações conceituais muito simples, como o CERT da Segurança e Indústria, na sua obra “Resiliência: aproximação a um marco de medição” (2018) contempla:

> Quando um sistema é capaz de suportar todo tipo de pressões sem mudar seu comportamento, sendo assim robusto. Quando um sistema não é capaz de suportar mais pressões, pero pode integrar mudanças para diminuí-las e pode seguir adiante, então é ciber-resiliente (p. 11, tradução nossa).

O termo resiliência cibernética vem sendo utilizado fortemente tanto seja no âmbito empresarial quanto nas políticas dos estados na manutenção (ou aprimoramento) da sua efetividade. Um exemplo disto é a existência da plataforma digital da empresa FM Global Companhia de Seguros Comerciais, cujo objetivo é assegurar a continuidade dos negócios e a proteção de bens dos clientes por meio da prevenção de riscos e coberturas de seguro.

Dentro de sua plataforma digital essa empresa apresenta um mapa global com os índices de resiliência. Mesmo aqueles índices de medição para estabelecer a classificação estabelecida para cada país em quanto ao maior ou menor nível de resiliência sejam limitados só aos aspectos economia, qualidade de risco e cadeia de suprimentos, representam um exemplo concreto da relevância do termo, como é o caso da estratégia para combater o flagelo imperante no âmbito cibernético e a abrangência de nível estratégico que pressupõe.

GRÁFICO 1 – *FM Global Resilience Index*.



Fonte: FM Global (2019).

Já no setor estatal e internacional, retomando o raciocínio da Estônia e da OTAN, é possível perceber como a responsabilidade dos governos no âmbito cibernético é um assunto complexo e que supera amplamente os interesses das corporações privadas. Mesmo assim, o trabalho entre o privado e o público, nacional e internacional, civil e militar, nesta área, se traduz em uma condição necessária para alcançar a efetividade desejada.

Por meio desta integração é que se conseguiu ver materializada a recuperação da Estônia depois do ataque cibernético sofrido, graças às medidas adotadas por aquele país, pela OTAN e, posteriormente, pelo CCDCOE.

A partir da análise bibliográfica abordada na pesquisa, das medidas adotadas pela Estônia e OTAN entre 2007 e 2019, e das considerações que poderiam ter sido tomadas, foi criada uma lista de possíveis condicionantes. Tudo isto, convenientemente amparado pela literatura, será norteado pelo emprego da ferramenta metodológica denominada *Process Tracing* (mapeamento ou rastreamento de processos), em procura da criação de um possível modelo de resiliência cibernética.

Enquanto a essa técnica, Rodrigues e Rodrigues (2017) definem que o *process tracing* "consiste em um conjunto de ferramentas e testes para investigar inferências causais a partir de dados qualitativos" (p. 2). Em tanto, à luz de Amorim Neto e Rodrigues (2016), podem se distinguir dois passos no método: o primeiro procura a identificação das causas principais (ou suficientes) as quais devam dialogar com as condições necessárias; e o segundo procura instrumentar as medidas para sua identificação. Como o foco do presente estudo é a identificação das causas principais para a constituição de um possível sistema cibernético resiliente fazendo uma análise histórica de 2007 até 2019 no âmbito da OTAN, o primeiro passo foi abordado com detalhamento, deixando a instrumentação das medidas para futuros estudos.

Com a intenção de aprofundar o modelo deduzido, foram submetidas todas as condições levantadas à análise de 58 especialistas que deram sua visão quantitativa e qualitativa da problemática, para estabelecer uma causas necessárias, suficientes, INUS e SUIN segundo a categorização que Mahoney (2015) faz ao respeito.

Finalmente, a fim de trazer à América do Sul aportes que signifiquem uma evolução na matéria, se pretende transferir aquelas políticas de resiliência cibernética aplicáveis no âmbito da OTAN na América do Sul (UNASUL, PROSUL, OEA), empregando o fundamento teórico denominado *policy transfer (*transferência de políticas).

A Transferência de Políticas é entendida como um processo em que o conhecimento dos programas, disposições administrativas, instituições e do sistema político permitem o desenvolvimento de características similares em outro ambiente (BENSON, 2000).

Acrescentando essa visão, a história demonstra que um modelo aplicável a uma determinada região pode não dar certo em outra por questões tanto endógenas como exógenas desse ambiente. É por isso que, empregando o conceito de transferência de políticas, e tomando como referência Dolowitz e Marsh (2000), se pretende transferir esse padrão à América do Sul.

Apesar deste modelo possível advindo da Estônia gerar resiliência em outras partes do globo, pode não ser factível na América do Sul. Em termos de gestão e acesso a recursos materiais, humanos e financeiros, nem sempre é possível desenvolver a plenitude de modelos complexos.

QUESTÃO DE ESTUDO

A formulação de uma teoria deve ocorrer por meio da elaboração de um problema, redigido de maneira precisa, com o intuito de ser submetido ao teste científico (CHALMERS, 1999). Para tanto, a problematização se caracteriza pelo enunciado, claro e explícito, acerca da dificuldade que o pesquisador pretende solucionar (RUDIO, 1978). Sob este prisma, no âmbito desta pesquisa, a problematização será apresentada da seguinte maneira:

A partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernético da OTAN, quais são as condições necessárias que conduzem à resiliência de sistemas cibernéticos e como estas práticas podem se transferir no âmbito da América do Sul?

OBJETIVOS

À guisa de colimar os esforços da pesquisa, em prol de uma resposta à questão de estudo, foi delineado um objetivo geral para nortear o processo de investigação, conforme enunciado abaixo:

Objetivo Principal: Compreender, a partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernético da OTAN, quais são as condições necessárias que conduzem à resiliência de sistemas cibernéticos e como estas práticas podem se transferir no âmbito da América do Sul.

No intuito de auxiliar na consecução do objetivo geral, foram delineados objetivos específicos, à luz de um encadeamento lógico, para nortear as ações que serão realizadas na dimensão estrutural da pesquisa, conforme a sequência abaixo.

- Objetivo Específico 1: Compreender o princípio da resiliência e seus componentes essenciais como alvo a ser atingido pela OTAN na sua estrutura cibernética.

- Objetivo Específico 2: Delinear quais são os elementos constituintes de sistemas resilientes e suas respectivas relações de necessidade e suficiência.

- Objetivo Específico 3: Analisar em que medida estes parâmetros internacionais foram ou podem ser importados pela América do Sul de maneira efetiva, conforme a literatura de transferência de políticas.

DELIMITAÇÃO DO ESTUDO

A presente pesquisa abrange a descrição da evolução da Estônia como modelo de sistema da OTAN, quanto à segurança e defesa cibernética, bem como a relevância que o Centro de Excelência Cooperativo de Defesa

Cibernética tem para essa região. A descrição conceitual de termos relacionados ao tema é necessário para a concepção do objeto de estudo, identificação e aplicação dos elementos condicionantes essenciais para a implantação de um sistema ciber-resiliente, juntamente com um modelo aplicável à problemática proposta, com a avaliação da possibilidade (ou não) à América do Sul.

Somente serão abordados aspectos referidos à OTAN e América do Sul, considerando neste último caso as organizações UNASUL, já em extinção, o PROSUL, como novo órgão regional em desenvolvimento, e a OEA como organismo macro que envolve todo o continente, não realizando abordagens particularizadas dos países contidos nessas estruturas.

No que se refere à análise da Estônia e à consequente evolução doutrinária, será considerado exclusivamente o período de 2007 a 2019, além dos aspectos fundamentais que constituem contribuição essencial para o problema proposto.

Finalmente, serão catalogadas as diferentes condições que, segundo a bibliografia consultada, respondem à necessidade ou não de que um sistema seja considerado ciber-resiliente. Isto para o modelo a ser criado seja alterado só a partir da opinião de especialistas a serem consultados.

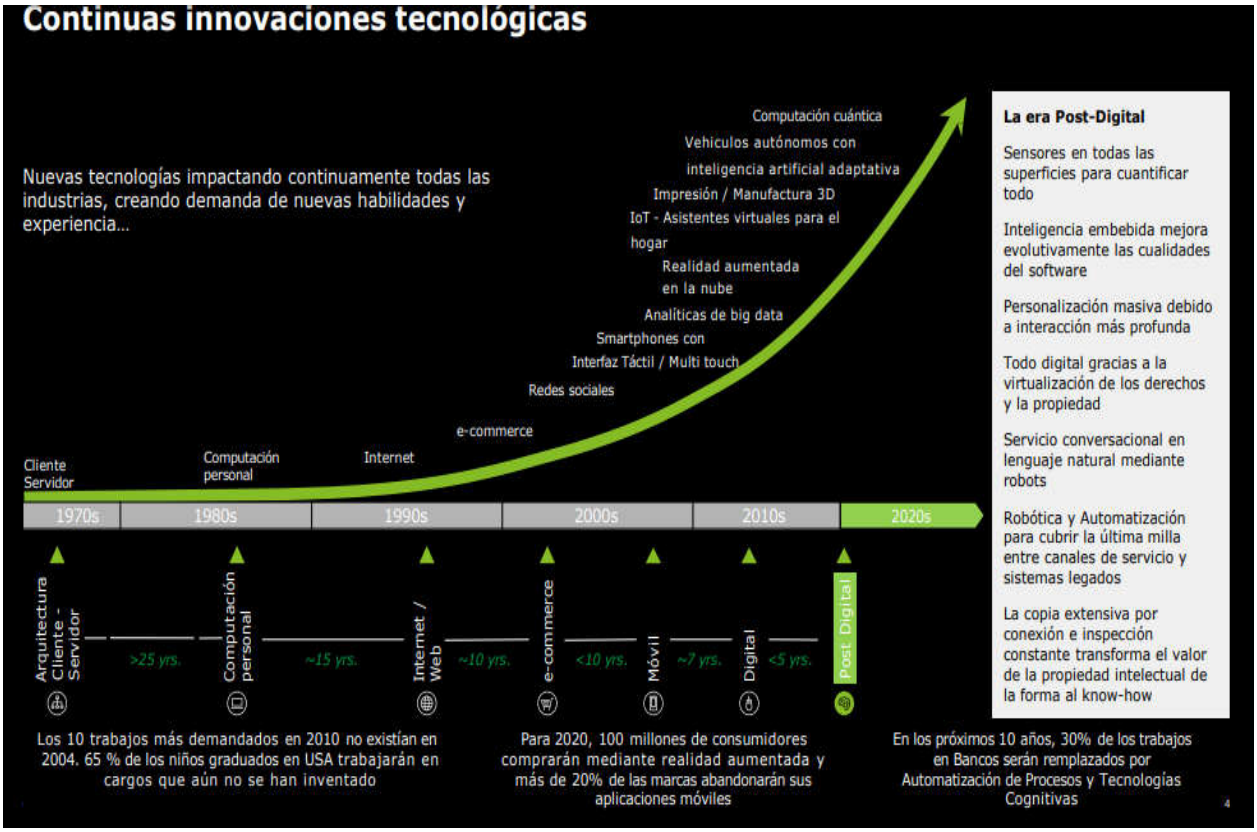
RELEVÂNCIA DO ESTUDO

O mundo de hoje está passando por uma profunda crise digital, dada a esmagadora evolução dos sistemas de computadores, a interligação de todos os tipos de dispositivos e a confluência de informações de forma indiscriminada por meios que nos últimos tempos seriam impensáveis.

Caso incorporemos nestas problemáticas intenções maliciosas de todos os tipos de agentes (pessoas, robôs, organizações, etc), o diagnóstico situacional é caótico, especialmente quando se trata de um espectro pouco explorado como a cibernética.

Analisando as projeções que a organização Deloitte (2019) apresenta como evolução contínua das inovações tecnológicas, a complexidade das operações no espaço cibernético exigirá ainda maior dificuldade.

GRÁFICO 2 – Evolução das Inovações Tecnológicas



Fonte: Castellanos (2019), p.4.

Nesta representação é possível perceber como a curva da complexidade da era pós-digital impacta continuamente todas as indústrias, criando demanda de novas habilidades, experiências e, sobretudo, maior segurança cibernética.

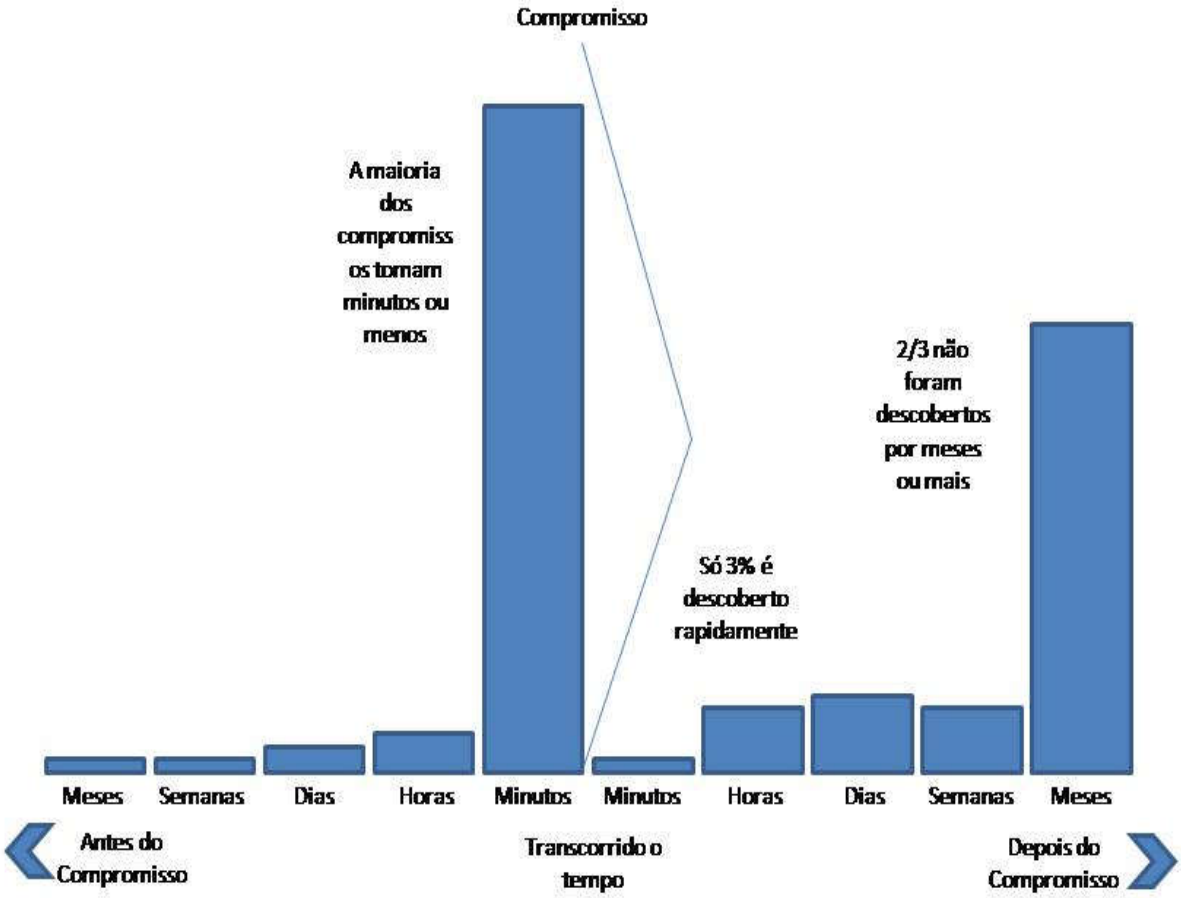
O mesmo informe coloca em foco principal a resiliência cibernética como um dos pilares de maior importância para fazer frente aos novos desafios e não perder a efetividade das organizações.

A partir desta realidade, é preciso reduzir a brecha entre o ataque cibernético e a resposta correspondente. Esse é um dos aspectos mais fortemente procurados pela resiliência cibernética, sendo então um dos fundamentos da relevância da presente pesquisa científica.

A seguir, se apresenta um gráfico fornecido pela mesma organização apresentada precedentemente (DELOITTE) aos efeitos de manter o raciocínio apresentado no informe de referência. Neste gráfico, exportado pelo autor (CASTELLANOS, 2019) do *Verzion Data Breach Investigations Report 2018*, é explorada a ideia que "a brecha existente entre a velocidade em que se completam os ataques e os tempos de resposta das organizações constitui um

dos principais desafios das organizações atuais em matéria de resiliência Cibernética" (p. 22, tradução nossa).

GRÁFICO 3 – Brecha entre Ataque e Resposta

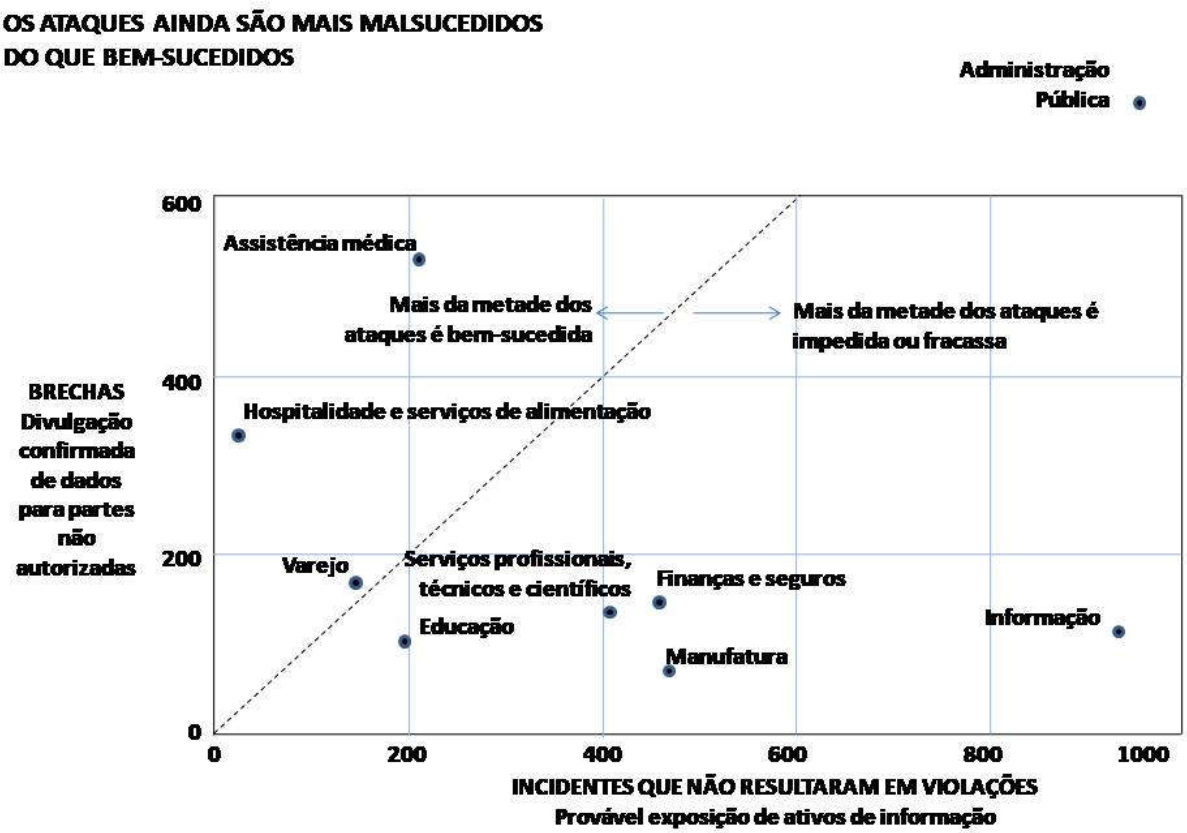


Fonte: Castellanos (2019), p.22. Tradução e adaptação própria.

Mesmo assim, as estruturas cibernéticas ainda têm uma vantagem para ser explorada: os ataques cibernéticos ainda são predominantemente malsucedidos.

Tomando como referência um estudo disponibilizado pela *Harvard Business Review* na sua edição para o Brasil, os autores Berinato e Perry (2018) apresentam um gráfico explicativo que justifica o que foi falado no parágrafo precedente.

GRÁFICO 4 – Eficiência dos ataques cibernéticos na atualidade



Fonte: Berinato e Perry (2018).

Isto quer dizer que ao desafio próprio das ameaças cibernéticas no futuro imediato, com a evolução das técnicas, táticas e estratégias, as ameaças poderão ser mais concretas e dificultosas, provocando a necessidade de que haja estratégias próprias adaptáveis e essa complexidade.

Continuando com esse raciocínio, se apresenta a seguir o Informe de Exploração de Perspectivas de Futuro (2018), fornecido pelo *Business Continuity Institute*. Ele pressupõe que o uso da internet para ataques mal-intencionados (ataques cibernéticos) será a maior ameaça nas perspectivas futuras, seguido da perda de empregados relevantes nas organizações, tudo bem mais abaixo as mudanças climáticas.

Isto permite inferir que a problemática cibernética continuará nas agendas públicas, privadas, nacionais, internacionais, regionais e globais.

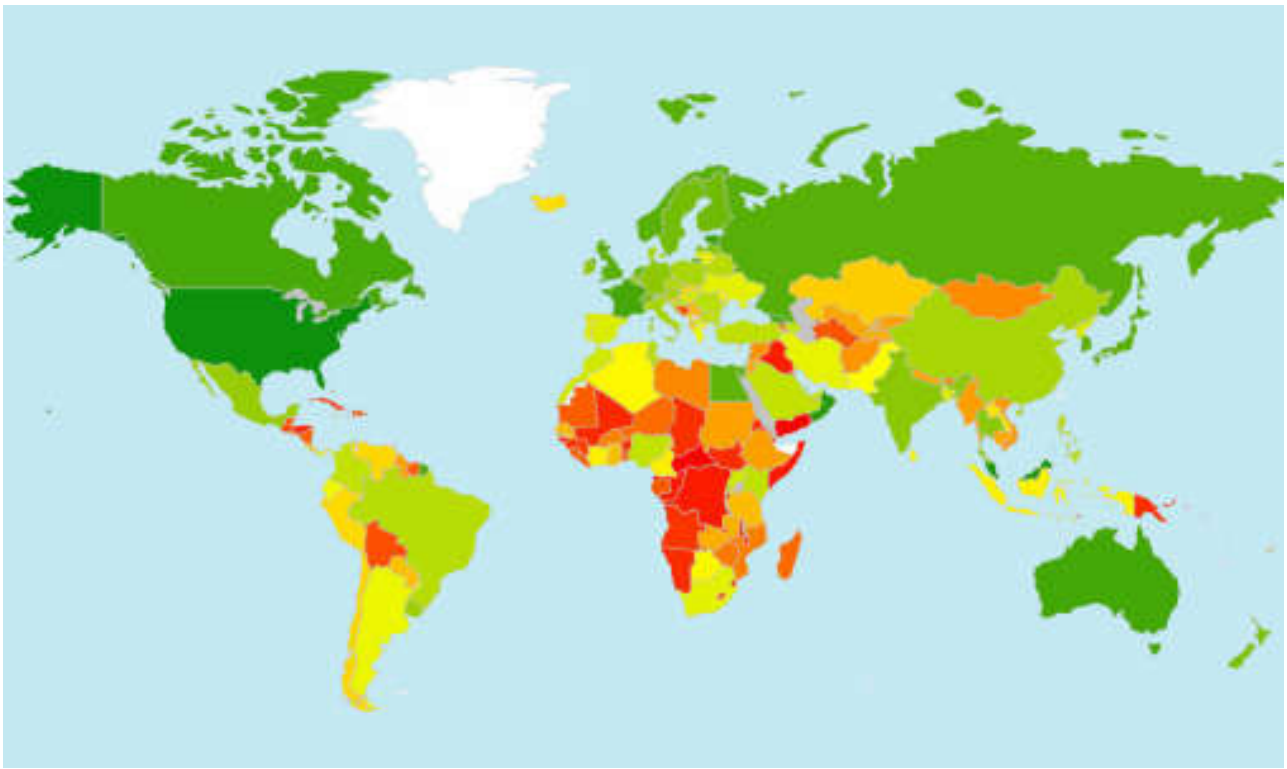
Como primeira conclusão desse informe, se estabelece que:

> Os incidentes cibernéticos permanecem com a preocupação maior tanto ao longo como ao curto prazo. Os ataques cibernéticos a grande escala que se tem apresentado nos últimos doze meses, assim como o número crescente de dispositivos contados na Internet, reafirmam a necessidade de construir organizações cibernéticas resilientes (BCI, 2018, p. 26, tradução nossa).

Entendendo que, a partir das experiências adquiridas pela Estônia quanto à resiliência cibernética, a OTAN está impondo medidas como norma de funcionamento cibernético na Europa, será possível apreciar que cada um desses componentes do modelo precisa ser devidamente analisado e compreendido para facilitar sua aplicação fora desse ambiente controlado.

Como fundamentos ao exposto, serão trazidos os chamados "Resultados Chave" elaborados pela *International Telecommunications Union* (ITU), no seu *Global Cyber Security Index* 2017 (GCI). Neste relatório, se representa graficamente a grande variedade de compromissos de segurança cibernética. No mapa será possível identificar de verde escuro os países com maior nível de compromisso e em vermelho mais forte, os de menor compromisso.

GRÁFICO 5 – Mapa com o nível de compromisso em segurança cibernética



Fonte: ITU - Global Cyber Security Index (2017), p. 13.

Sendo assim, a América Latina é menos consciente dessa cultura cooperativa e colaborativa que possibilite a aplicação de medidas no campo cibernético que contribuam à blindagem da região como um todo. Isto se contrasta com o que acontece hoje, estando cada país agindo em relação a sua particularidade geopolítica.

O presente estudo é relevante por quanto procurará identificar as condicionantes necessárias e suficientes para construir um sistema cibernético resiliente no âmbito da América do Sul, avaliando as práticas do Centro de Excelência Cooperativo de Defesa Cibernético da OTAN, na Estônia. Ressalta-se que na transferência de políticas públicas nem sempre é possível copiar práticas aplicadas em outros estados nação ou entidades supranacionais.

Somado a isso, permitirá avaliar e ponderar o peso que é dado às resoluções regionais da OTAN para a aplicação de medidas no campo cibernético.

A respeito da relevância dos dados obtidos, não se limitará às conclusões do autor, mas também se amparará em especialistas na matéria para, junto com eles, chegar a um modelo de resiliência cibernética aplicável no conglomerado de variáveis e condições, além de sua devida catalogação.

Finalmente, dos resultados obtidos e da análise da situação regional em termos da evolução do domínio da defesa do ciberespaço e da cooperação nesta matéria, se avaliará a possibilidade (ou não) de aplicação de um modelo cibernético exportável de uma situação, um contexto diferente e mais evoluído.

ESTRUTURA DA PESQUISA

Esta dissertação foi estruturada no formato monográfico, constituído por uma introdução e quatro capítulos, elaborados progressivamente e de forma encadeada, com o intuito de prover sinergia à investigação e, assim, alcançar os objetivos propostos. Neste sentido, a introdução e os capítulos foram estruturados à pesquisa conforme o descrito abaixo.

Introdução: Nesta seção são abordadas a introdução, a questão de estudo, o objetivo principal e os objetivos secundários identificados para serem atingidos, a delimitação do estudo, a relevância e estrutura de pesquisa.

Capítulo 1: Referencial Teórico e Metodológico. Neste capítulo procurou-se abordar todo o referencial teórico como fundamento acadêmico à pesquisa. Assim, foram analisados inicialmente os conceitos e definições referentes à resiliência, cibernética, espaço cibernético, guerra cibernética, segurança cibernética, defesa cibernética e antifragilidade.

Seguidamente foram analisados os conceitos de cooperação e integração internacional. A compreensão desses termos e conceitos é fundamental para entender as medidas que a OTAN está adotando no marco regional e influindo no marco global. Sendo uma das intenções da pesquisa a transferência do modelo criado no âmbito da América do Sul, a cooperação e integração internacional não podem ficar ausentes do marco teórico referencial.

Referido à metodologia, além de desenvolver o tratamento e a coleta de dados, foi realizado um detalhamento da metodologia de pesquisa com que cada capítulo será abordado.

Capítulo 2: A OTAN e a Ciber-Resiliência. O objetivo desse capítulo é compreender o princípio da resiliência e seus componentes essenciais como alvo a ser atingido pela OTAN na sua estrutura cibernética.

Os conteúdos a serem tratados serão: a evolução da Estônia no campo cibernético até o ataque cibernético massivo de 2007, para entender o contexto geral do acontecido; as medidas adotadas pela Estônia e pela OTAN após os ataques cibernéticos de 2007, para materializar a celeridade da reação de um país submetido a um ataque cibernético massivo, e como o conceito de cooperação e integração se aplicam e beneficiam o desenvolvimento do conjunto; os componentes essenciais que poderiam transformar um sistema cibernético vulnerável, em resiliente, a partir da exploração bibliográfica e o entendimento das diversas medidas que vem se implantando na Europa na matéria; aplicando o mapeamento de processos (*process tracing*) como técnica para a criação de um mecanismo causal sustentado em um contexto histórico.

Capítulo 3: Procurando um modelo Ciber-Resiliente. O objetivo desse capítulo é delinear quais são os elementos constituintes de um sistema cibernético resiliente e suas respectivas relações de necessidade e suficiência. Por isso, cada uma das condições foi submetida a uma avaliação dos expertos e especialistas que conceituarão seu grau de importância (1 a 7) a partir da formulação de questionários. Esta será a parte quantitativa da pesquisa. A

partir da análise dos dados coletados, as condições causais serão identificadas (necessárias, suficientes, INUS e SUIN).

Capítulo 4: É Possível uma América do Sul Ciber-Resiliente? O objetivo é analisar em que medida estes parâmetros internacionais foram ou podem ser importados pela América do Sul de maneira efetiva, considerando como organismos regionais a UNASUL, o PROSUL e a OEA, conforme a literatura de transferência de políticas (*policy transfer)*.

Para atingir esse padrão de desempenho foram abordados os seguintes conteúdos: análise da situação particular da América do Sul em quanto às organizações que poderiam concentrar esforços no estabelecimento de medidas projetadas no ambiente cibernético e favorecer a cooperação regional. Para isto se apresentam as seguintes organizações:

- UNASUL, já em processo de desarticulação, mas com diretrizes relativas à defesa cibernética elaboradas e implementadas, as quais poderiam servir de base para futuros convênios com outras organizações.

- PROSUL, criado em março de 2019, sem nenhum desenvolvimento, mas que poderia absorver algumas das responsabilidades assumidas pela UNASUL.

- OEA, sendo esse um organismo de maior envergadura regional, com vasta experiência quanto à cooperação e integração dos países das Américas.

Este capítulo continua-se com o estudo bibliográfico e documental para entender a realidade quanto à integração e cooperação da região, para após isso submetê-lo à teoria de transferência de políticas públicas.

Conclusões: nesta parte final da pesquisa, abordam-se os seguintes pilares para atingir no padrão desejado: (1) a relevância que tem o princípio da Resiliência no campo cibernético baseado na experiência obtidas pela Estônia na sua evolução digital; (2) a importância do CECCD OTAN para alcançar um modelo de resiliência cibernético de nível regional; (3) a Cooperação Europeia para o estabelecimento de padrões de excelência necessários para atingir a resiliência cibernética; (4) os resultados de pesquisa realizada com especialistas sobre um modelo de resiliência cibernética aplicável no marco do conglomerado de variáveis e condições, e sua devida catalogação para formar um mecanismo causal que permita chegar à formação de um modelo aplicável de resiliência cibernética; (5) o peso que é dado às resoluções regionais da

OTAN para a aplicação de medidas no campo cibernético; e (6) a possibilidade (ou não) de aplicação de um modelo cibernético exportável de um contexto diferente e mais evoluído.

A fim de arrumar as idéias, acompanhar o raciocínio e tentar não perder a orientação da pesquisa, foi desenhado e aplicado um esquema gráfico que norteou todo o processo de investigação (**APÊNDICE A** – Esquema Gráfico de Pesquisa).

1. REFERENCIAL TEÓRICO E METODOLÓGICO

1.1 REFERENCIAL TEÓRICO

Dada a complexidade da dimensão na qual a presente pesquisa se insere, é necessário enquadrar alguns conceitos fundamentais para o melhor entendimento de dita problemática. Sendo que o essencial da pesquisa é a possibilidade de construção de um modelo de resiliência cibernética, o primeiro conceito a ser abordado será a “resiliência“ propriamente dita, dentro de sua ampla abrangência relativa ao âmbito de aplicação.

Sua origem vem da física, sendo definida pelo Estrada (2017) como a “energia de deformação (por unidade de volume) que pode ser recuperada do corpo deformado quando cessa o esforço que causa a deformação” (p. 30, tradução nossa). O mesmo autor diz, em outras palavras, que seria seu limite elástico. Ou seja, “uma vez superado esse limite, o material já não se pode recuperar e fica deformado” (p. 31, tradução nossa).

Grotberg (2005) entende que a resiliência é “a capacidade humana para enfrentar, vencer e ser fortalecido ou transformado por experiências de adversidade” (p. 15, tradução nossa), evidenciando-se uma perspectiva eminentemente afetiva do termo, enquanto Infante (2005), a define como “uma resposta global em que estão em jogo os mecanismos de proteção, entendendo por estes não a valência contrária aos fatores de risco, mas aquela dinâmica que permite ao indivíduo sair fortalecido da adversidade, em cada situação específica, respeitando as características pessoais” (p. 25, tradução

nossa), sendo esta uma definição orientada não só à dimensão afetiva, mas também procedimental.

Como foi abordado no início do capítulo, esse conceito tem uma grande abrangência de vertentes, produto da sua versatilidade de aplicação. A partir disto é que se tentará afunilar o conceito até chegar a um censo comum de definição.

Já no contexto organizacional, Poletti e Dobs (2007) consideram que a Resiliência é “um conjunto de qualidades que favorecem o processo de adaptação criativa e transformação a despeito dos riscos e adversidades” (p.13, tradução nossa), entanto Tavarez (2001) afirma que “a resiliência é a capacidade de responder de forma mais consistente aos desafios e dificuldades do mundo, reagindo com flexibilidade e capacidade de recuperação diante desses desafios e circunstancias desfavoráveis, tendo uma atitude otimista, positiva e perseverante” (p.35, tradução nossa).

Outra vertente diferente seria a que o Melillo (2005) apresenta, citando diversos autores relevantes que propõem definições de resiliência, sendo a de Vanistendael bastante acertada respeito ao que pretende com a presente pesquisa. Ele distingue dois componentes que deve ter a resiliência dependendo do contexto, sendo o primeiro diante da destruição, gerando a capacidade de se proteger a integridade sob pressão, e o segundo, além da resistência, a capacidade de construir uma visão positiva apesar das circunstancias difíceis.

Como foi possível apreciar, o emprego do conceito de resiliência depende da estratégia empregada pelo indivíduo que queira fazer uso dela, mas a definição que será considerada como válida aos fins da pesquisa será a formulado pelo CERT da Segurança e Indústria, na sua obra “Resiliência: aproximação a um marco de medição” (2018):

> Quando um sistema é capaz de suportar todo tipo de pressões sem mudar seu comportamento, sendo assim robusto. Quando um sistema não é capaz de suportar mais pressões, pero pode integrar mudanças para diminuí-las e pode seguir adiante, então é ciber-resiliente (p. 11, tradução nossa).

Continuando com o raciocínio, a seguinte concepção a ser tratada será a de “cibernética”, já que constitui a chave essencial onde inserir o princípio de resiliência supracitado.

Sendo a cibernética um termo que nos dias atuais resulta de simples dedução por ter relação direta com a informática e as redes e por nos encontrarmos na “Era da Informação“, serão apresentadas a seguir duas definições de autores renomados que possuem contrapontos, aspecto este que permitirá ao leitor construir um mais aprofundado entendimento do conceito.

Assim, Stel (2005), ao referir-se à aplicação da cibernética, diz que “inclui a psicologia, a inteligência artificial, a economia, a engenharia de sistemas de controle de organismos vivos, máquinas e organizações“ (p.14, tradução nossa), destacando que, “ao se pôr em movimento, a informação se transforma em uma atuação ou resultado desejado“ (p.14, tradução nossa).

Por sua parte, Van Creveld (2010), com uma visão logicamente orientada ao âmbito militar, diz que:

> A cibernética e os computadores trouxeram algo mais que câmbios na administração, a logística, as comunicações, a inteligência e as operações, também ajudou a que um novo conjunto de pessoas, pessoas que pensavam na guerra e que planejavam, livravam e avaliavam, puderam se encarregar disto com a ajuda de novos critérios e desde um ponto de vista totalmente novo (p. 246, tradução nossa).

Dessa maneira, Stel faz ênfase na importância que tem a cibernética na tomada de decisão influenciando todos os componentes de um sistema, e Van Creveld coloca o foco na mudança que a cibernética tem gerado em todas as ordens da campanha. Entanto, qualquer um dos conceitos apresentados deixa claramente evidenciada a importância da cibernética no mundo atual.

Nesse sentido, a cibernética se insere em um novo ambiente que é chamado de “espaço cibernético“, o qual também tem inúmeras definições que, em seu conjunto, permitem o concreto entendimento desse termo.

Começando com Clark e Knake (2011) eles afirmam que o espaço cibernético está conformado por “todas as redes informáticas do mundo e todo o que elas conectam e controlam, não só internet “(p.104, tradução nossa). Acrescenta essa definição dizendo que o espaço cibernético é “internet mais

outras tantas redes de computadores às que se supõe, não é possível acessar desde internet“ (p.104, tradução nossa).

Continuando essa sucinta análise, verifica-se a necessidade de avançar nas definições, abordando uma visão mais direcionada à macroeconomia dos Estados. Assim, Sierra (2015) define o espaço cibernético como “o conjunto de meios e procedimentos baseados nas TIC configurados para a prestação de serviços“ (p.16, tradução nossa). O mesmo autor também faz uma abordagem referente a sua constituição, dizendo que é conformado pelo “hardware, software, internet, serviços de informação e sistemas de controle que garantam a provisão de aqueles serviços essenciais“ (p.16, tradução nossa).

Por sua vez, Williams (2014), a partir de um detalhamento quase excessivo da abrangência do termo, refere-se ao espaço cibernético como:

> O domínio artificial criado ao conectar todos os ordenadores, computadores, roteadores, cabos de fibra óptica, dispositivos sem fios, satélites, e outros componentes que nos permitam mover grandes quantidades de dados a velocidades muito rápidas. Da mesma maneira que nos domínios físico, terrestre, marítimo, aéreo e espacial, no espaço cibernético levamos a cabo uma variedade de atividades em benefício de indivíduos, governos e entidades comerciais. A diferença clave entre os domínios físicos e o espaço cibernético é que o espaço cibernético é artificial e cambiante. Essa característica oferece tanto oportunidades quanto riscos (p. 14, tradução nossa).

Desde uma visão mais estratégica (de segurança de um Estado), Llongueras Vicente (2013) define o ciberespaço como “um elemento de poder dentro da segurança nacional“ (p.1, tradução nossa). Essa definição, contundente por seu conteúdo e relevância para o âmbito cibernético, se sustenta na sua ideia de que é um novo domínio artificial que exerce uma grande influência estratégica na nossa Era, distinguindo a ideia de que atores mais modestos podem se constituir em ameaças para as grandes potências, e que essa assimetria se sustenta no novo conceito de operações militares centradas em redes.

Entrando, no âmbito militar e de segurança, segundo o Informe da Estratégia de Segurança Nacional dos Estados Unidos do ano 2010, a

importância do espaço cibernético é tal que tem sido definido como um novo "*Global Commons*" (USGovernment, 2011).[3]

Finalmente, Ottis e Lorents (2012), oferecem um componente ainda não citado nas definições precedentes, sendo considerado pelo autor como imprescindível para a correta compreensão do espaço cibernético. Os autores consideram o espaço cibernético como um conjunto de sistemas de informação interconectados dependentes do tempo, onde os usuários interagem com outros sistemas. Os autores trazem o tempo como condição diferenciadora das outras definições apresentadas, já que, comparando com outros sistemas dependentes do tempo se observa que, no espaço cibernético, podem ocorrer mudanças radicais em curto tempo.

Perante os argumentos expostos, é possível afirmar que a definição de Williams (2014), mesmo sendo muito detalhada em alguns casos, adicionando ao conceito de tempo proposto por Ottis e Lorents (2012), constitui a conjunção de conceitos mais acertados para explicar o espaço cibernético.

Outro termo que deriva e decanta logicamente desta abordagem teórica é o conceito de Guerra Cibernética que, segundo Stel (2005), poderia ser definida como o emprego das Forças Armadas no ambiente cibernético contra outro ator em um cenário de conflito, “para atacar sistemas, redes e instalações informáticas e de comunicações“ (p.11, tradução nossa).

Esse mesmo autor adiciona à definição apresentada que o enfrentamento no ciberespaço traz implícito o emprego da força convencional para complementá-lo.

Por seu turno, Conti e Surdu (2009) abordam a necessidade da capacidade e criatividade humana para o sucesso das ações cibernéticas, estabelecendo como premissa que esse tipo de guerra requer “não só de habilidade técnicas, mas também de habilidades para solucionar os problemas de criatividade, para atuar de maneira equilibrada sobre pressão e de pensamento crítico“ (p.17, tradução nossa).

---

3 *Global Commons*: espaços que, sem ser de soberania de uma nação em particular, podem ser aproveitados em benefício próprio por qualquer ator, conforme às regras concretas aceitadas internacionalmente.

Com uma visão mais pragmática do assunto, Nye e Welch (2013) definem a guerra cibernética como uma ação hostil no ciberespaço cujos efeitos ampliam ou são equivalentes a uma violência física relevante, demonstrando um propósito manifesto de deixar claro o quão devastador pode ser uma guerra no ciberespaço.

Como acompanhamento essencial do termo guerra cibernética vêm os conceitos de Segurança Cibernética e Defesa Cibernética, os quais serão abordados nessa mesma ordem.

Relacionado com o termo segurança cibernética a bibliografia é muito ampla, sendo possível perceber sua evolução conforme a avaliação do conceito. Na atualidade é necessário estabelecer definições padronizadas por órgãos internacionais, com ingerência na matéria, para aprimorar o emprego correto deste termo.

Assim, por exemplo, Kemmerer (2003) afirmava que a segurança cibernética consistia, em grande medida "na utilização de métodos defensivos para detectar e frustrar possíveis intrusos" (p. 707, tradução nossa). Em verdade, essa definição na atualidade é mais aplicável à segurança informática do que à segurança cibernética.

Nessa questão, destaca-se Lewis (2006), ao enfatizar que a segurança cibernética implica a proteção de redes informáticas e a informação contida nela. Esse autor começa a introduzir, também, os conceitos de danos maliciosos e intrusões, mas sem o aprofundamento necessário, ao menos na definição.

No cenário temporal de 2008, o órgão denominado *International Telecommunication Union* – ITU, dependente da Organização das Nações Unidas, determinou uma definição de segurança cibernética na Recomendação UIT-T X.12052 (2008), aprovada em Resolução 1813 (2010), que estabelece:

> A segurança cibernética é o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, métodos de gestão de riscos, ações, formações, práticas idôneas, seguros e tecnologias que podem se utilizar para proteger os ativos da organização e dos usuários no entorno cibernético. Os ativos da organização e os usuários são dispositivos informáticos conectados, os usuários e os serviços / aplicações, os sistemas de comunicações, as comunicações multimídias, e a totalidade da informação transmitida e / ou armazenada no entorno cibernético. A segurança

> cibernética garante que sejam alcançadas e mantidas as propriedades de segurança dos ativos da organização e os usuários contra os riscos de segurança correspondentes no entorno cibernético.

Com o avanço paulatino do termo e a abrangência cada vez maior do conceito, a Relatoria Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos (CIDH), da Organização dos Estados Americanos (OEA) estabeleceu no documento Liberdade de Expressão e Internet (2014), como salvaguarda da população, que:

> O conceito de segurança cibernética habitualmente é empregado como um termo amplo para se referir a diversos temas, desde a segurança da infraestrutura nacional e das redes a través das quais se prove Internet, até a segurança ou integridade dos usuários. Mesmo assim, desenvolvimentos posteriores sugerem a necessidade de limitar o conceito exclusivamente ao resguardo dos sistemas e dados informáticos.

Por sua parte, Newmayer (2015) define o termo segurança cibernética como “o conjunto de práticas políticas, de treinamento e tecnologias desenhadas para proteger o entorno cibernético com a finalidade de asgurar a integridade da informação“ (p.78, tradução nossa).

No cenário contemporâneo*, The Information Systems Audit and Control Association* – ISACA (2018) aborda uma definição de segurança cibernética que se orienta à proteção de ativos de informação a través do tratamento de aquelas ameaças que poderiam colocar em risco qualquer informação processada, armazenada e transportada pelos sistemas de informação.

Assim, a *ISSO 27001,* referindo-se à acepção de ISACA (2018), define Ativo da Informação como: "conhecimento ou dados que têm valor para uma organização"; e Sistemas de Informação como: "os que compreendem as aplicações, serviços, ativos de tecnologias da informação ou outros componentes que permitem o manejo da mesma".

Sendo o turno agora da Defesa Cibernética, poderia se disser que começa a ser definida no âmbito da OTAN em 2010, particularmente em novembro desse ano, quando os Ministros de Defesa dos países-membros, em conferência, aprovaram a definição e, em junho de 2011, a política de defesa cibernética e um Plano de Ação de Defesa Cibernética.

A definição sobre Defesa Cibernética estabelecida pela OTAN, conforme o – *MC0571-NATO Cyber Defence Concept* – com referência no *National Cyber Security Framework Manual* (2012) foi: "a aplicação de medidas de segurança para proteger as infraestruturas críticas dos sistemas de informação e comunicações frente aos ataques cibernéticos" (p. 181, tradução nossa).

Esse mesmo documento afirma que a defesa cibernética constitui um âmbito de segurança nacional no qual os estados deverão tomar determinadas medidas, em todos os estratos (público e privado), tanto seja para delitos como para garantias e liberdades individuais, para responder a todo tipo de agressões, estabelecendo sistemas de resposta e cooperação.

O tratamento mais recente do conceito de defesa cibernética está sendo abordado pelo *Centro Conjunto de Desarrollo de Conceptos* (CESEDEN) do Estado-Maior da Defesa no Reino da Espanha. O CESEDEN (2018) definiu o seguinte:

> Considera-se imprescindível dar uma resposta global e integral para o conjunto das Forças Armadas, e para o Ministério da Defesa em geral, em linha com o desenvolvimento das vigentes políticas do departamento e em estreita coordenação com os organismos responsáveis da provisão de serviços e na operação e manutenção de redes e sistemas, que permita fazer frente de forma eficaz aos importantes desafios que se fazem frente neste âmbito. A ciberdefesa como capacidade militar, deve estar plenamente integrada em todos os âmbitos das Forças Armadas e do Ministério da Defesa em geral, assim como com o resto dos atores civis e militares do âmbito nacional e internacional, com quem se compartilham riscos e ameaças. Por outro lado, se considera o fator humano como chave do êxito, referidos no só ao pessoal técnico e operativo envolvido nas atividades do ciberespaço, mas também com todo usuário dos serviços que se proporcionam a través de redes e sistemas (p.6, tradução nossa).

O mais importante deste parágrafo apresentado, denominado "*Idea Central: Integración*", que não traz a definição acabada do termo, é a abrangência da problemática, no nível nacional e internacional, público e privado, individual e coletivo, civil e militar. Esse será um dos enfoques mais relevantes, levados em consideração neste trabalho acadêmico.

O mesmo CESEDEN (2018), como conclusão, estabelece que o conceito de defesa cibernética desenvolvido é só uma guia para fazer frente às capacidades militares e organização das Forças Armadas no âmbito

cibernético. Conceitos relevantes como esses tem que ser aprofundados nas seguintes fases de planejamento e implementação.

Dessa maneira uma interpretação clara, à luz das definições ministradas, indica que a defesa cibernética e a segurança cibernética não podem ser atividades isoladas, mas sim devem estar inclusas na defesa nacional e, por tanto, na defesa militar, na proteção de infraestruturas críticas e sistemas de comando e controle.

Outro conceito emergente, não tão explorado ainda, mas que não pode ser deixado fora desse referencial teórico por sua relevância, é a antifragilidade. Seu mentor é Nassim Taleb, quem propõe dois conceitos diferentes, mas intimamente relacionados: “Cisnes Negros” e “Antifragilidade”.

No caso dos ¨Cisnes Negros¨, Taleb (2010) entende que são eventos aleatórios, caóticos e incertos de efeitos extremos e transcendentes, podendo ser eles de origem natural e/ou antrópico.

A “Antifragilidade” é definida por Taleb (2012) como a capacidade de certos sistemas fazerem frente e se beneficiarem, assimetricamente, dos Cisnes Negros.

Assim, o mesmo autor conclui que a antifragilidade oferece uma estratégia que resolve sistematicamente o problema da fricção e a incerteza própria do enfrentamento entre vontades inteligentes.

Segundo Borgoñón (2017), a antifragilidade, como atributo desejável de um sistema:

> “É a medida da liberdade de ação e fuga da interdependência de uma organização ou organismo complexo, que a adota como estratégia para articular o propósito emergente da entidade do sistema com a disposição e capacidade dos meios em oportunidade (tempo, espaço e ritmo) frente a exposição de ações intrínsecos e extrínsecos heterogêneos de origem natural e/ou antrópicos, com o objeto de se beneficiar dos efeitos convexos assimétricos. Assim, uma ação do ambiente ou do oponente, que por suas qualidades é incerta e volátil, constitui uma opção que fortalece o próprio sistema de maneira assimétrica. Em analogia, a fragilidade constitui um atributo desejável para aquele sistema complexo que opera como oponente e impede ao próprio sistema o logro dos seus propósitos” (p. 34, tradução nossa).

Borgoñón (2017) também afirma que fornecer aos sistemas organizacionais militares atributos de antifragilidade implica necessariamente

adotar uma inter-relação e interdependência heterogênea e diversa na sua dimensão informacional.

Dada a complexidade que esse conceito representa para padronizar processos que favoreçam à resiliência, não será abordado no presente trabalho constituindo só um conceito mais do arcabouço de conhecimentos necessários para o entendimento da área.

Entrando já no referencial estrutural do estudo, serão abordados termos tais como cooperação e integração, assuntos esses que representam pilares estruturais para a construção do conhecimento pretendido na presente pesquisa.

Começando com a análise, a Agência Peruana de Cooperação Internacional (2010) considera a cooperação internacional como um conjunto de ações e ferramentas de caráter internacional a movimentar recursos e intercambiar experiências para alcançar metas comuns. Distingue também diversos critérios a serem tidos em conta para a constrição daquela cooperação, tais como: solidariedade, equidade, eficiência, sustentabilidade e interesse mútuo.

Outro conceito intimamente relacionado com a cooperação é o Desenvolvimento, a partir do lançamento do Programa de Nações Unidas para o Desenvolvimento (PNUD).

Relacionado a isto, Sunkel e Paz (1981) afirmam que a cooperação internacional é partícipe ao desenvolvimento, da seguinte forma:

> "[...] crescimento, o processo de câmbio estrutural global, a concepção do desenvolvimento humano, a teoria da eleição racional, entre outras [...] Neste sentido, ao analisar a Cooperação Internacional, deve-se fazer, sobre uma clara concepção do Desenvolvimento de um país e os esforços próprios que como tal faz para lográ-lo [...]" (p. 15, tradução nossa).

Portanto, a cooperação internacional não significa que o ator com maior desenvolvimento vai proteger e ajudar necessariamente ao ator menos desenvolvido. Muito pelo contrário, o sistema internacional de cooperação exige que os atores façam esforços para lograr as metas estabelecidas e assim criar as condições para que essa cooperação seja viável.

Para ampliar os conhecimentos, agora com o conceito de Integração, Puchala (1972) a define como um "conjunto de processos que produzem um sistema de concordância de nível internacional, no qual os agentes encontram possibilidades de harmonizar coerentemente seus interesses" (p. 181, tradução nossa).

Como contraponto à visão anterior, Caporaso e Pelowski (1975) consideram que "a integração consiste na emergência de novas estruturas e funções em um novo nível dos sistemas, mais abrangente que os anteriores" (p. 421, tradução nossa), entanto Contreras (1993) afirma que integração, no sentido estrito, consiste em que "a través dos tratados internacionais, dois ou mais estados cedem algumas das suas prerrogativas soberanas para criar uma zona jurídica independente à dos seus membros" (p. 40, tradução nossa).

Nesta última definição o autor centra sua atenção na cessão da soberania e o processo de integração para alcançar essa integração. O interessante destas definições é que permitem inferir o período histórico no qual foram construídas.

Por outra parte, Treto (2002) estabelece que:

> A integração regional é um processo político, econômico, social e cultural amplo, profundo e multifacetado, mediante o qual dois ou a econômica e política e fomentando os intercâmbios entre suas sociedades e, ao mesmo tempo, vão cedendo gradualmente suas atribuições soberanas no nível supranacional de governabilidade, com a participação de atores governamentais e não governamentais, seus sistemas sociais e culturais e seus mecanismos de defesa e segurança, sem perder por aquilo sua identidade nacional própria maximizando os benefícios e minimizando os custos da interdependência e globalização (p. 47, tradução nossa).

Fazendo uma analogia entre as duas últimas definições, é possível perceber como o conceito de integração é amplamente aprofundado por sua relevância, além de mitigar a problemática da soberania que tanto preocupava no século XX.

Consequentemente, pode se disser que existe uma relação direta entre a integração e a soberania, sendo que essa última está reconhecida como princípio do Direito Internacional, em conformidade com a Carta das Nações Unidas (Resolução 2625 da Assembléia Geral das Nações Unidas), a qual estabelece que "todos os Estados gozam de igualdade soberana, têm direitos e

deveres iguais e são membros congêneres da comunidade internacional, em que pese às diferencias de ordem econômica, social, política ou de qualquer outra índole" (p.95, tradução nossa).

1.2 METODOLOGIA

Nesta seção será apresentada a metodologia aplicada à tentativa de responder os problemas delineados na pesquisa, identificando as atitudes necessárias para atingir os objetivos elencados. Para isso haverá uma sequência organizada em: Tratamento dos Dados e Coleta de Dados.

Portanto, utilizando a taxonomia de Vergara (2008), por meio de uma pesquisa essencialmente exploratória, procurou-se compreender as evidências da situação do estado da arte na Estônia (particularmente o Centro de Excelência Cooperativo de Defesa Cibernética da OTAN) referida ao ambiente cibernético, a necessidade de entender e criar um modelo de resiliência cibernética à luz das experiências refletidas neste caso, e a possibilidade (ou não) de exportar esse modelo à América Latina.

Neste sentido, e sendo que a metodologia aplicada o que pretenderá é a criação de um possível modelo (ou sistema) de resiliência cibernética, resulta conveniente abordar antecipadamente esses conceitos.

Shannon (1988) define Sistema como um conjunto de objetos ou ideias que estão inter-relacionadas entre elas, como uma unidade para a consecução de um fim. Sendo essa uma definição clássica mais ampla, abordaremos a visão do Ladrière (1978) ao respeito, que a define como:

> Uma entidade ideal que possui eventualmente certa estrutura interna que pode se caracterizar, em geral, no curso do tempo e que é susceptível de se encontrar, em cada instante, em um estado inteiramente analisável em princípio. O possuir uma estrutura interna significa que pode se descompuser em outros subsistemas; além de possuir os diferentes indivíduos ou elementos que o conformam, uma série de funções e relações (p. 39, tradução nossa).

Sendo claramente entendido o conceito de sistema, é o turno agora do modelo. Villaplana (2012) faz uma abordagem afastada do tratamento técnico da problemática, mas absolutamente pertinente, clara e considerada da definição:

> O termo modelo é polissêmico pelo que dá lugar a ambiguidades. Algumas de suas conotações não são relevantes para o processo de investigação, pois não são usos técnicos no sentido epistemológico. Cotidianamente costuma-se falar de modelo como um objeto que se reproduz ao imitá-lo; por exemplo, um patrão de costura ou um bordado. Outro sentido comum faz referência à amostra de um produto que se expõe para sua venda ou às pessoas que os exibem. No plano ético, significa procurar de uma perfeição ideal, de um comportamento ou modo de vida, mas sem chegar a alcançá-lo, como no caso da namorada ou do aluno ideal. No campo artístico se refere às pessoas, paisagens, animais e objetos que intentam reproduzir-se (p. 8, tradução nossa).

Levando em consideração termos mais técnicos, Wartofsky (1983) considera que um modelo é uma "versão derivada ou representada de algo tomado do original; a nova entidade se produz ao imitar o original" (p. 190, tradução nossa), alinhado isto com a visão do Bravo (1998) quem afirma que "na perspectiva epistemológica o modelo pode se considerar como uma espécie de descrição ou representação da realidade [...]" (p. 130, tradução nossa).

Continuando o raciocínio, Ladirère (1978) afirma que "a construção do modelo está dirigida por certa preconcepção da realidade estudada" (p. 39, tradução nossa). Segundo Bravo (1988), "o modelo, frequentemente, é suscetível de sistematização" (p. 131, tradução nossa).

O mesmo autor afirma que "o modelo se constitui como um método para auxiliar o estudo da realidade e contribuir com a compreensão das teorias e das leis, servindo em alguns casos para verificá-las" (p. 131, tradução nossa).

Apoiando a visão anterior, Bisquera (1989) afirma que "o modelo tem um caráter instrumental" (p. 44, tradução nossa), senda essa última a ração principal da relevância do presente estudo.

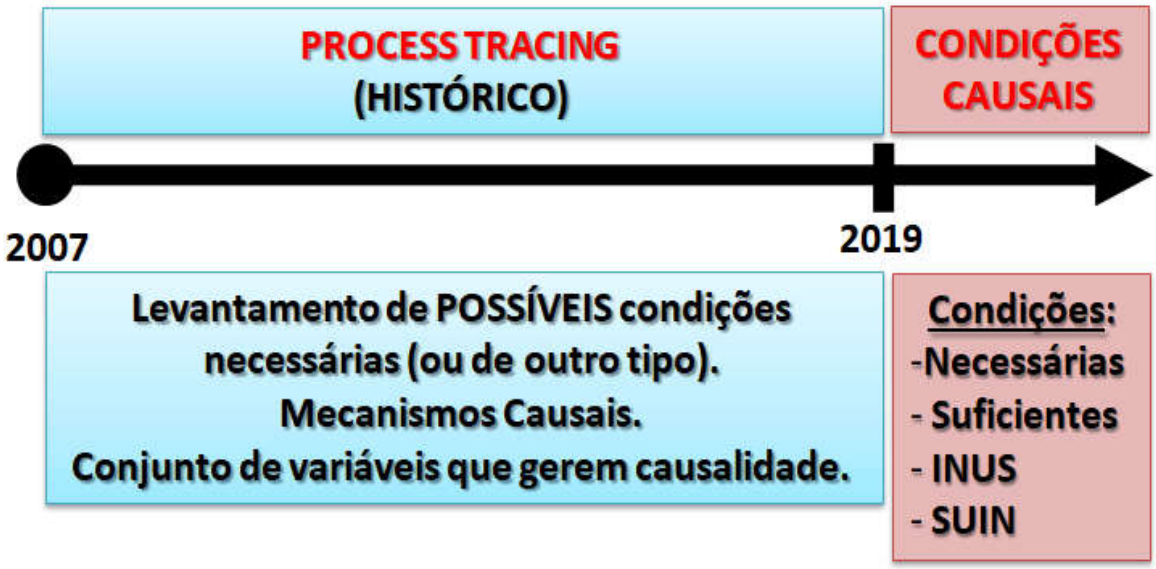
1.2.1 TRATAMENTO DOS DADOS

Para cumprir com os objetivos fixados, e de acordo com a estrutura da pesquisa já apresentada, a abordagem metodológica será estruturada em função do conteúdo de cada capítulo.

Primeiro Capítulo (Marco Referencial Teórico e Metodológico): No caso desse capítulo, a abordagem será eminentemente qualitativa contemplando como premissas a subjetividade, a descoberta, a valoração do entorno, procurando-se entender os fenômenos, privilegiando a história e a análise dos documentos, empregando como procedimento técnico a pesquisa bibliográfica, a qual se baseia na análise de material já publicado.

No gráfico seguinte apresenta-se uma esquematização do tratamento dos dados nos capítulos segundo e terceiro:

GRÁFICO 6 – Esquematização do tratamento dos dados nos capítulos segundo e terceiro



Fonte: O Autor.

Segundo Capítulo (A OTAN e a Resiliência Cibernética): Neste capítulo, como se procura o entendimento de fenômenos complexos específicos, em profundidade, mediante descrições e interpretações, sem considerar os seus aspectos numéricos em termos de regras matemáticas e estatísticas, será empregada a metodologia qualitativa.

Para isso será conduzida inicialmente uma pesquisa exploratória como primeira aproximação com o tema e com os fatos e fenômenos relacionados ao problema a ser estudado. Permitirá determinar as relações existentes além de permitir o conhecimento do tipo de relação.

De maneira complementar, neste capítulo, se executará uma pesquisa explicativa para expor os (aspectos) determinantes para a ocorrência de um fenômeno, processo ou fato (condicionantes para constituir um sistema cibernético resiliente), sendo esta uma consequência lógica da pesquisa exploratória.

Procura-se explicar a relação entre a causa e o efeito no marco histórico, empregando a técnica metodológica de *process tracing* para compreender assim o mecanismo causal[4] resultante.

Segundo Rodrigues e Rodrigues (2017):

> O *Process Tracing* emerge como método para se auferir o poder explicativo de estudos históricos através da sistematização clara das evidências, seguindo alguns preceitos contidos na tradição quantitativa, abrangendo questões como a equifinalidade, gerando explicações para mecanismos causais e validando hipóteses. Em última instância, consiste em um conjunto de ferramentas e testes para investigar inferências causais a partir de dados qualitativos (p. 2).

Os resultados gerados por um mecanismo dependem fundamentalmente do contexto em que opera. Então, sequência distintas dos mesmos tipos de elementos constituem contextos distintos, os quais podem gerar resultados distintos, a pesar do mesmo mecanismo estar em ação em todos os contextos em tela.

Terceiro Capítulo (Procurando um modelo de Resiliência Cibernética): Neste capítulo se apresenta para o pesquisador o maior desafio desde o ponto de vista metodológico, a partir da combinação de metodologia quantitativa e qualitativa no mesmo assunto, e a ferramenta de análise de Mecanismos Causais como fechamento do capítulo.

Iniciando com uma abordagem quantitativa, a partir do trabalho com variáveis (condicionantes) expressas sob a forma de dados numéricos (valoração de especialistas) e emprego de técnicas estatísticas para classificá-los e analisá-los (tabela de valores).

---

[4] Segundo Aguirre (2017) ″um mecanismo causal constitui uma representação teórica sobre processos empíricos e complexos que permitem sugerir uma relação de causalidade que, de fato, pode apelar explicitamente a entidades, ações, processos ou associações meramente conjeturais″ (p. 155).

A materialização desta parte da pesquisa será efetuada a partir de elaboração de um questionário de pesquisa (**APÊNDICE B** – Processo de Elaboração do Questionário) distribuído numa população de 58 especialistas em defesa cibernética, em 15 países.

O questionário de pesquisa abrange todos os condicionantes levantados como possíveis componentes a serem considerados dentro de uma condição causal que poderia gerar resiliência, contendo aqueles questionários uma parte quantitativa, a partir de perguntas com uma gradação de 1 até 7 pontos de relevância, respondendo às premissas próprias da escala de Likert[5], e outra qualitativa, deixando a possibilidade aos especialistas de transmitir suas opiniões ao respeito (**APÊNDICE C** – Questionário de pesquisa).

Essa parte qualitativa da pesquisa será também de ordem analítica, sendo que envolve uma avaliação mais aprofundada das informações coletadas no estudo (a partir da avaliação dos condicionantes por parte de especialistas), na tentativa de explicar o contexto do fenômeno estudado.

Amparados na literatura do Mahoney (2015), poderia se disser que se distinguem as seguintes condições categorizadas dentro dessa ferramenta (condições causais):

a. Condições Necessárias (mas não suficientes): Presença ou ausência do resultado que se deseja explicar. Proposição segundo a qual um resultado não teria ocorrido na ausência dela, mas também que sua presença não bastaria para garantir o resultado.

b. Condições Suficientes (mas não necessárias):Sua presença garante a concretização ou consumação do resultado que se deseja explicar. A presença de tais condições significa a existência do resultado.

c. INUS: Parte insuficiente, mas necessária, de uma condição que é ela mesma não necessária, mas suficiente para o resultado. Ou seja, não é nem necessária nem suficiente.

---

[5] O criador dessa escala foi Rensis Likert, quem publicou em 1932 um informe onde descrevia seu uso. É uma escala métrica comumente utilizada em questionários e é a escala de uso mais amplo nos questionários para pesquisa, principalmente nas ciências sociais (SANCHEZ, 1993).

d. SUIN: Causa que é parte suficiente, mas não necessária, de um fator que é insuficiente, mas necessário, para um resultado.

Quarto Capítulo (É Possível uma América do Sul Ciber-Resiliente?): Finalmente neste capítulo será realizada novamente uma abordagem qualitativa, empregando uma metodologia de pesquisa documental (analisando documentos conservados nos órgãos públicos e privados de qualquer natureza) e bibliográfica (analisando material publicado em livros, revistas, jornais, redes eletrônicas e material acessível ao público em geral).

Acompanhando esse processo, será efetuada uma pesquisa exploratória como primeira aproximação do pesquisador ao tema, e consequentemente explicativa com o objetivo central de explicar os fatores determinantes para a ocorrência do fenômeno ou fato, que neste caso seria a possibilidade (ou não) de transferir o modelo criado à luz da OTAN na América do Sul, visando explicar o porquê das coisas.

1.2.3 COLETA DE DADOS

Exclusivamente para o terceiro capítulo, particularmente no emprego do questionário como ferramenta metodológica para a pesquisa (quantitativa), serão coletados os dados a partir da distribuição de um questionário para especialistas na área da cibernética. Os resultados obtidos serão analisados para arribar a conclusões de relevância.

Os especialistas serão um total de 58, pertencentes a 15 países, os quais representam os seguintes continentes e subcontinentes: América do Sul, América Central, América do Norte, Europa, Ásia e África.

Aos efeitos de dimensionar o esforço de coleta de dados para a pesquisa, será apresentado um mapa, identificando a origem dos profissionais que contribuíram com o trabalho de campo:

GRÁFICO 7 - Representação geográfica do esforço de coleta de dados da pesquisa

Fonte: O Autor.

2. A OTAN E A RESILIÊNCIA CIBERNÉTICA

2.1 EVOLUÇÃO DE ESTÔNIA NO CAMPO CIBERNÉTICO ATÉ O CIBERATAQUE MASSIVO DE 2007

Segundo os registros históricos existentes e fornecidos pelo *Institute of the Estonian Language*, a Estônia começou a trabalhar no âmbito cibernético pelos 1965, com a instalação do computador URAL-1, na escola de ensino médio *Nõo High School*, na cidade de Nyo. Nessa época, a Estônia estava ainda sobe dominação da União Soviética e esse foi o primeiro projeto de educação informatizada feito pela União Soviética nesse país.

Nesse caminho, a evolução continuou e em 1967 a Universidade Tecnológica de Tallinn recebeu seu primeiro computador Minsk 22, também de origem soviético, no ano 1982 foi instalado o primeiro computador na

universidade de Tartu, e em 1990, pessoal do Instituto de Cibernética, já usava correios eletrônicos (AVIAR, 2007).

Jordan (2003) afirma que em 1989 foi introduzido o sistema de redes para computadores FidoNet, empresa construída em base a uma cooperativa de comunicações. Para o ano 1990 a FidoNet já tinha ao redor de 30.000 sistemas de computadores conectadas com quase 1,56 milhões de usuários.

Nesse mesmo período, a rede soviética RELCOM (*Reliable Comunications*), fez a conexão entre servidores da Estônia e servidores da Finlândia, sendo o verdadeiro ícone de desenvolvimento e salto tecnológico o ano 1991, oportunidade em que foi declarada a Independência da República da Estônia. Com isto, logo surgiu uma radical modernização da infraestrutura de telecomunicações nacionais.

Para Garcia-Ajofrin (2016), a partir desta situação, o processo de digitalização da Estônia começa a crescer chegando em 1996 a implantação do projeto de inovação chamado de Salto do Tigre, o qual procuraria incrementar os investimentos em tecnologias da informação e as comunicações no nível nacional levando, entre outros sucessos, a que o sistema educativo do país esteja apoiado na internet a partir do fornecimento de computadores em todas as escolas, objetivo que foi alcançado no ano 2000.

Segundo o *Wiley Handbook of Science and Technology for Homeland Security* (2010), no ano 2006 teria lugar o estabelecimento do *Computer Emergency Response Team for Estony* (CERT-EE). A função principal desse órgão seria a gestão das incidências de segurança no domínio ".ee".

Mas toda essa evolução tecnológica teria sido afetada de maneira massiva o dia 26 de abril de 2007, a partir de uma série de ataques cibernéticos perpetrados após a decisão do governo da Estônia de tirar o monumento ao Soldado de Bronze de Tallinn, monumento que significava a passagem e influência da então União Soviética pelos países Bálticos.

Outro aspecto relevante que levanta Ferrero (2013) é referido ao desagrado Russo produzido pela incorporação da Estônia na OTAN em 2004.

Czosseck, Ottis e Taliharm (2011) descrevem que o período em que a Estônia foi submetida aos ataques cibernéticos foi entre o dia 27 de abril e 18

de maio de 2007, se distinguindo duas fases, uma no começo das operações, entre 27 e 29 de abril, caraterizada por ter sido utilizadas ferramentas rudimentares contra sítios web principalmente governamentais no Ministério da Defesa, estruturas do estado e partidos políticos; e outra fase desde o 30 de abril até o 18 de maio, com ataques cibernéticos mais complexos e coordenados.

A partir dos acontecimentos sofridos, o apoio internacional na Estônia chegou desde seus aliados OTAN e desde a União Europeia, dando cumprimento ao estabelecido no Tratado de Washington (ou Tratado do Atlântico Norte), datado em 4 de abril de 1949.

Assim, podem se destacar nos artículos 4 e 5 desse tratado:

> - Artículo 4: As partes de consultarão quando, a juízo de quaisquer delas, a integridade territorial, a independência política ou a segurança de qualquer das partes fosse ameaçada.
>
> - Artículo 5: As partes convêm que um ataque armado contra uma ou mais delas, que tenha lugar na Europa ou na América do Norte, seja considerado como um ataque dirigido contra todas elas, e em consequência, acordam que se tal ataque se produz, cada uma delas, em exercício do direito de legítima defesa individual e coletiva reconhecido pelo artigo 51 da Carta das Nações Unidas, ajudar à Parte ou Partes atacadas, adotando seguidamente, de forma individual e de acordo com as outras Partes, as medidas que julgue necessárias, incluso o emprego da força armada, para restabelecer a segurança na zona do Atlântico Norte. Qualquer ataque armado desta natureza e todas as medidas adotadas em consequência serão imediatamente colocadas em conhecimento do Conselho de Segurança. Essas medidas acabarão quando o Conselho de Segurança tenha tomado as disposições necessárias para restabelecer e manter a paz e a segurança internacional.

Sendo que esses tipos de ataques ainda não se encontravam devidamente definidos (enquanto se eram ou não uma ação militar), a resposta dos países envolvidos no Tratado não foi imediata nem impositiva. Inicialmente a ajuda veio anulando ações de softwares maliciosos, e depois disso cresceu com um fornecimento gradual de maior largura de banda, com a precaução de não liberar demais essa capacidade para evitar ser afetados também pela ação cibernética do agressor.

Finalmente, Ferrero (2013) afirma que "o ataque cibernético à Estônia em 2007 significou um marco histórico para a OTAN e pode ser considerada como a primeira ação de ciberguerra" (p. 93, tradução nossa), deixando claramente

evidenciada a magnitude desse acontecimento. Esse mesmo autor afirma também que representou a primeira ocasião em que um estado-membro solicitou apoio à OTAN pela afetação da sua infraestrutura crítica de informação. Foi nesta circunstancia também que foi demonstrado que a OTAN não tinha plano de ação para contingências cibernéticas, o que gerou a elaboração de um informe de lições aprendidas por dita organização.

2.2 MEDIDAS ADOTADAS PELA ESTÔNIA E PELA OTAN APÓS OS ATAQUES CIBERNÉTICOS DE 2007

Já para 19 de maio o ataque cibernético tinha finalizado, deixando como protagonistas um atacante desconhecido e uma vítima totalmente clara e identificada. Mesmo não tendo comprovado um responsável, o Ministro das Relações Exteriores da Estônia (Urmas Paet) deu como fato que esse agressor tinha sido a Rússia, não deixando lugar a dúvida nenhuma ao respeito da postura estônica do assunto. Essa acusação foi negada pelas autoridades russas, fato que se mantém até nossos dias (AVIAR, 2007).

Segundo o informe surgido do Comitê de Bucarest do dia 3 de abril de 2008[6], em referência à reunião dos Ministros da Defesa dos países da OTAN, em Bruxelas, no dia 14 de junho de 2007, a necessidade que foi vista nessa época de trabalhar conjuntamente no marco da defesa cibernética foi o que levou à organização ao estabelecimento de medidas cooperativas nessa área.

O artigo 47 desse informe estabelece:

> A OTAN continua empenhada em fortalecer os principais sistemas de informação da aliança contra ataques cibernéticos. Adotamos recentemente uma Política de Defesa Cibernética e estamos desenvolvendo as estruturas e autoridades para realizá-la. Nossa Política de Defesa Cibernética enfatiza a necessidade de que a OTAN e as nações protejam os principais sistemas de informação de acordo com suas respectivas responsabilidades; compartilhar as melhores práticas; e fornecer uma capacidade para ajudar as nações aliadas, mediante solicitação, a combater um ataque cibernético. Esperamos continuar o desenvolvimento das capacidades de defesa cibernética da OTAN e fortalecer as ligações entre a OTAN e as autoridades nacionais.

---

[6] *Issued by the Heads of State and Goverment participating in the meeting of the North Atlantic Council in Boucharest on 3 April 2008*

A partir do enunciado anteriormente, é que começam a ser desenvolvidas as medidas de cooperação cibernéticas, como foi o caso, conforme ao exposto por McNamara (2010), da criação do Centro de Coordenação de Defesa Cibernética, chamado de “Defesa do Tigre”, tendo como base a Estônia, principal interessado em que isto aconteça.

É assim que Taddeo e Giorioso (2017) fazem uma cronologia do que seria posteriormente a criação do Centro de Excelência Cooperativo de Defesa cibernética – CECCD (corretamente denominado em inglês *Cooperative Cyber Defence Center of Excellence – CCDCOE*), com data de abertura o 14 de maio de 2008, sendo os países que deram início a esta organização a Alemanha, a Eslováquia, a Espanha, a Estônia, a Itália, a Letônia e a Lituânia, alcançando cinco meses depois o status de Organização Militar Internacional.

Mas a organização continuou crescendo conforme a evolução do pensamento nesta área e aos riscos que evidentemente foram se reconhecendo desta nova dimensão da guerra, incorporando-se em 2010 a Hungria, em 2011 os Estados Unidos e a Polônia, em 2012 a Holanda, e em 2014 a Áustria (sendo que esse país não é membro da OTAN), a França, o Reino Unido e a República Checa.

Dito crescimento não foi só no âmbito militar, econômico, político e tecnológico, mas também legal, como o detalha Ziolkowski (2013). O autor explica que em 2009, na cidade de Tallinn, começa a ser desenvolvido um manual que nesse mesmo ano teve sua primeira versão (Manual Tallinn[7]). O que se procurou com esse documento é, a partir das boas práticas no campo da cibernética, e das experiências adquiridas, estabelecer, à luz das bases legais vigentes, normas de conduta e procedimentos a abordar em caso de um ataque cibernético.

Tikk, Kaska e Vihul (2010) em um trabalho minucioso realizado sobre as considerações legais de incidentes cibernéticos internacionais, detalham que o Manual Tallinn procurou (e procura) encontrar uma harmonia entre o Direito

[7] O Manual Tallinn é um documento acadêmico, não vinculante, que trata sobre a aplicabilidade da lei internacional nos conflitos no âmbito cibernético. Dito manual foi desenvolvido pelo comitê do CCDCOE da OTAN, na Estônia (SCHMITT, 2013).

Internacional e as responsabilidades dos Estados, tendo em conta que os conflitos cibernéticos e essa nova dimensão desconhecida não estava sujeita a normativa nenhuma que os respalde, tentando, desta maneira, gerar uma referência, um nexo que lhes permita dar um tratamento comum às problemáticas geradas ao respeito.

Estrada (2017) deixa em evidência que o ataque cibernético recebido pela Estônia teve impacto mundial, permitindo à sociedade digital tomar conta à sociedade digital da nova ameaça e da necessidade de os países cooperarem e se tornarem proativos ante um problema que chegou para ficar, tomando como exemplo a Estônia, que conseguiu se adaptar e superar rapidamente à adversidade, sendo na atualidade um dos países com maior penetração da internet no mundo, e que pode fazê-lo depois que sofreu em 2007, porque criou as condições necessárias para cooperação regional além de ter criada uma devida consciência situacional na população.

2.3 COMPONENTES ESSENCIAIS QUE PODERIA TRANSFORMAR UM SISTEMA EM CIBER-RESILIENTE

Para entender as condições que levaram à Estônia a se constituir como um estado com um alto índice de ciber-resiliência, e sua consequente projeção aos países da Europa, a partir das diretrizes estabelecidas pela OTAN, baseadas nas boas práticas do Centro de Excelência Cooperativo de Defesa Cibernética de dita organização, é preciso identificar primeiro as variáveis que possibilitaram articular esse modelo e o mecanismo causal que gerou essa eficiência, particularizando cada causa componente segundo a sua relevância.

Mesmo tendo identificadas variáveis, das condições causais que a literatura identifica como necessárias para obter essa resiliência, quais são as que conduzem à resiliência de um sistema cibernético? Essa é a grande pergunta que deve ser respondida para criar o modelo de resiliência desejado.

A partir de um process tracing histórico das medidas adotadas tanto seja pela Estônia quanto pela OTAN entre o período 2007 até 2019, e das considerações que se inferem poderiam ter sido tidas em conta pela Estônia e o Centro de Excelência Cooperativo de Defesa cibernética da OTAN, foi criada

uma lista de possíveis condicionantes, convenientemente amparados pela literatura, que serão os que nortearão o processo de criação do mecanismo causal desejado.

Focados no contexto atual, tanto a OTAN quanto a UE tem se preocupado vigorosamente da resiliência, mesmo tendo essas duas organizações âmbitos de abrangência e responsabilidades diferenciadas.

A UE começou mais cedo que a OTAN na produção de documentos relativos à resiliência cibernética (ano 2012), sendo que a OTAN, mesmo no ano 2008 haja criado o CCDCOE, não tinha ainda produção documental, assunto esse que só no ano 2015 conseguiu resolver.

A UE tem se focado com maior ênfase, tentando melhorar a governança da estrutura no nível local e regional, estabelecendo três vetores amparados na Comunicação da Comissão ao Parlamento Europeio e ao Conselho, no dia 3 de outubro de 2012, chamada: o planejamento da UE sobre a resiliência e a redução do risco de catástrofes em países em desenvolvimento, aprendendo das crises alimentarias (UE, 2012). Ditos vetores são:

- Antecipar as possíveis crises por meio da avaliação de riscos, estabelecimento de sistemas de alerta e estreitamento de vínculos entre a informação adquirida, a elaboração e a tomada de decisões a nível nacional e regional.
- Prevenção e preparação, abordando as causas em profundidade referentes à fragilidade e a vulnerabilidade por meio de análises de risco.
- Melhorar a resposta à crise a traves da elaboração de um marco analítico conjunto, além de detectar as causas profundas, as incidências sobre os grupos de população afetados, avaliação das intervenções, identificando os âmbitos nos quais se maximizaria o impacto, definindo estratégias e prioridades de curto e longo preço, e divulgando experiências adquiridas em projetos exitosos.

É no ano 2013 que a UE lança seu Plano de Ação para a Resiliência 2013-2020 considerando que a resiliência é uma responsabilidade individual de

cada governo nacional e, por tanto, corresponda a cada um deles, definir as prioridades políticas, econômicas, sociais e médio-ambientais (UE, 2013).

Dito plano estabelece três fases: uma primeira que se orienta na preparação da sociedade para incrementar sua resiliência em questões como as infraestruturas, a segurança, os direitos humanos, as leis, os recursos, as instituições políticas, as comunicações, os abastecimentos, a energia, etc; uma segunda fase que pressupões a acontecimento do incidente cibernético, no qual são afetados os serviços levantados anteriormente, tentando nessa fase fazer frente ao desafio e adaptar-se a ele; e uma terceira fase na qual se pretende abordar uma recuperação paulatina tendente a alcançar no menor tempo possível os níveis perdidos com o incidente (UE, 2013).

Preliminarmente, e a partir da análise dos parágrafos supracitados, poderia se fazer uma aproximação, de maneira ainda muito incipiente, à distinção de algumas medidas a serem consideradas para construir o modelo de resiliência cibernética. Entre elas podem se destacar: a gestão de risco e de mudanças; o conhecimento profundo da organização para poder articular a medidas previstas na primeira e na segunda fase; a capacidade de antecipar a crise com organismos afins com essa função (CERT); a necessidade de um oportuno e adequado regulamento nas infraestruturas críticas; a determinação das previsões adequadas para garantir processos contínuos e operacionais em qualquer circunstância; a disposição de uma adequada estrutura de sistemas de informação (hardware e software); a pertinente adequação do quadro legal; a necessidade de cooperação privada, estadual, nacional e regional; a necessidade de adequar a formação e especialização do capital humano para fazer frente a esses novos desafios; e finalmente a implementação de estratégias de resiliencia nos níveis nacionais e regionais.

Continuando com a abordagem histórica de medidas adotadas na Europa para promover a resiliência cibernética, o primeiro documento que responde a essa temática é o denominado "*Strategic Foresight Analysis*", do ano 2015 (OTAN, 2015). Dito documento assinalou a questão da resiliência em zonas urbanas com uma problemática relevante para a segurança nacional tendo em vistas a crescente concentração de populações nas cidades.

Nessa mesma linha, em julho de 2016, é assinado no Comitê de Varsóvia, o ”Compromisso para fomentar a resiliência” (OTAN, 2016). Nessa reunião os mandatários se comprometeram em continuar fomentando medidas de resiliência contra as ameaças (inclusive híbridas) que provenham de qualquer direção, determinando-se que a resiliência resulta essencial para uma dissuasão e defesa acreditável.

Outro aspecto relevante surgido desse compromisso foi a assinatura do documento ”Requerimentos mínimos da OTAN para a resiliência nacional”, que estabelece sete grande áreas críticas (OTAN, 2016): continuidade dos governos, fornecimento de energia, serviços de comunicações civis, fornecimento de água e comida, capacidade para gerenciar grandes movimentos de população, capacidade para gerenciar grande número de vítimas, e sistemas de transporte civil.

Sendo que se considerou responsabilidade de cada nação a implementação de das medidas nas áreas supracitadas, foram estabelecidas as tarefas orientadoras dos esforços nacionais para alcançar os padrões de desempenho desejados (OTAN, 2017):

- Desenvolver recursos humanos para avaliar as vulnerabilidades nacionais (redes cibernéticas, infraestruturas críticas, infraestruturas de fornecimento de energia, etc).
- Desenvolver uma política cujo objetivo seja o planejamento e a gestão da resiliência de maneira coerente e que seja o suficientemente abrangente.
- Modificar a legislação para permitir maior flexibilidade de atuação dos governos em situação de crises.
- Melhorar a habilidade das empresas civis para fazer frente às crises.
- Avaliar os documentos de planejamento tendo em vista as novas ameaças.
- Estabelecer contato com outras organizações afins para coordenar a ação.

Mas de tudo o que foi apresentado até agora, o mais importante enquanto às funções da OTAN é a cooperação, assunto esse contemplado na

Declaração Conjunta de julho de 2016 (OTAN–UE, 2016). Neste documento são elencados os passo específicos para fomentar a cooperação entre a OTAN e a UE, sendo alguns deles a ciberdefesa, exercícios de treinamento, a gestão de crise, a cooperação propriamente dita, a pesquisa, a capacidade de defesa, entre outras tantas, sendo uma das principais o reforço da resiliência, de forma coordenada, com especialistas para apoiar aos estados membros da UE e aliados OTAN.

Entre as políticas de segurança que o documento apresenta, referidas à resiliência cibernética, poderias se elencar a definição do papel dos CERT, a definição de tarefas e missões dos operadores de infraestruturas críticas, o estabelecimento de padrões de segurança para o âmbito público e privado, as ajudas econômicas da OTAN e da UE aos países-membro que não posam alcançar os níveis desejados segundo os padrões de desempenho estabelecidos, entre outros (OTAN-UE, 2016a).

Finalmente, e a partir das informações apresentadas, poderiam ser levantadas as seguintes medidas essenciais a serem tidas em conta na formulação preliminar de um possível modelo de resiliência cibernética baseado nas experiências adquiridas pela OTAN (e UE) no período considerado:

- Gestão de risco e de mudanças.
- Conhecimento profundo da organização (interna e externamente).
- Área de Cibernética com capacidade e participação no nível da organização de gerenciamento e tomada de decisão.
- Capacidade de antecipar a crise (CERT).
- Simplificação de sistemas de informação para reduzir processos e interfaces.
- Processos contínuos e operacionais em qualquer circunstância.
- Garantir regulamentos nas infraestruturas críticas.
- Estrutura de sistema de informação (hardware e software).
- Desenvolvimento de exercícios e modelos de simulação.
- A atualização do quadro legal.
- Cooperação privada, estadual, nacional e regional.

- Ferramentas de desenvolvimento e melhoria contínua da segurança cibernética.
- A proteção física do patrimônio tecnológico.
- Formação e especialização de capital humano.
- Implantação e atualização das estratégias de resiliência cibernética.
- Dotação orçamental suficiente.

Considerando as condições levantadas, serão definidos a seguir os conceitos essenciais de cada uma delas â luz de referentes teóricos:

- Gestão de risco e de mudanças. Medidas preventivas e corretivas. Segundo Beaudoin, Japkowics e Matwin (2009), a gestão de risco atinge o equilíbrio certo entre o custo das medidas adotadas e o benefício hipotético para a sua implantação. Ou seja, este tipo de gestão é quando se trata de ameaças. O gerenciamento de mudanças se refere à identificação de mudanças a serem feitas e os impactos organizacionais que devem ser tidos em conta para o processamento adequado. Ou seja, este tipo de gestão é quando se trata da evolução da exposição a eventos externos. E as medidas preventivas são as decisões a serem adotadas como resultado da gestão de risco que não tem tido possível ser evitado ou que se tem previsto evitar no futuro, sendo que as corretivas são aquelas que são realizadas para eliminar a causa de um problema.
- Conhecimento profundo da organização (interna e externamente). Senge (2006) afirma que alcançar o conhecimento real e profundo da organização é uma condição fundamental. Resiliência cibernética requer adaptabilidade e sobrevivência, por isso, é necessário conhecer a organização e o ambiente. Visão crítica interna e externa da organização. A organização tem para programar redundância em seus sistemas, seus funcionários e seus processos. É para evitar expor cada um desses elementos da organização para a mesma ameaça. Em conclusão, o balanço de riscos entre todos os elementos da organização.
- Área de Cibernética com capacidade e participação no nível da organização de gerenciamento e tomada de decisão. Segundo o detalhe das partes componentes de uma organização e dos níveis que possui uma estrutura organizacional que estabelece Mintzberg (1989), se confere que, para

um sistema consiga atingir o seu estado de resiliência, é necessária uma liderança harmoniosa e sinérgica de todos os níveis e componentes da organização em causa. Requer-se de capacidade operacional no que se refere a medidas no campo cibernético (gestão de risco, mudança, medidas preventivas e corretivas), a sensibilização do pessoal e liderança adequada nos mais altos níveis da organização é necessária para trazer à realidade medidas a tomar.

- Capacidade de antecipar a crise (CERT). Segundo Newmayer (2015) essas capacidades são a chave para a resiliência. As Equipes de Resposta de Emergência (CERT) são compostas por especialistas em segurança cibernética e têm a responsabilidade de desenvolver preventiva e reativa a todos os tipos de incidentes relacionados à segurança dos sistemas informáticos.

- Simplificação de sistemas de informação para reduzir processos e interfaces. Analisando a teoria de Pelton e Singh (2015) a estrutura, a base de arquiteturas sistemas materiais e relações humanas devem ser tão simples quanto possível. Simplificar é um conceito que se refere a conseguir alguma coisa se torna mais simples, ou seja, menos complexa, difícil ou complicada. Dada a complexidade inerente aos sistemas informáticos, quanto mais simples sejam os sistemas, menores são os processos e interfaces, menos vulnerabilidades e violações de segurança serão geradas. Organizações mais simples são as que têm menos processos, em menos unidades, com menos sistemas, com menos interfaces entre eles.

- Processos contínuos e operacionais em qualquer circunstância. Segundo Estrada (2017), todo sistema informático é composto de infraestrutura, hardware, software e processos, cada um com um nível de interferência particularizado, afetando em maior ou menor medida, o bom funcionamento da plataforma. Mas todos eles trabalham sinergicamente para que, como um todo, possam se transformar em um sistema resiliente. Mas esse processo deve ser contínuo e operado sob quaisquer circunstâncias, distinguindo os processos que são essenciais e devem realizar escala de prioridades para o momento de ser temporariamente suspensos.

- Garantir regulamentos nas infraestruturas críticas. Os autores Rowland, Rice e Shenoi (2014), definem as infraestruturas críticas como aquelas

instalações, redes, serviços e equipamentos físicos e de tecnologia da informação cuja perturbação ou destruição teria um impacto maior sobre o funcionamento eficaz das instituições estatais e autoridades públicas. É por isso que é necessário que essas infraestruturas críticas sejam adequadamente reguladas e padronizadas para garantir a proteção necessária.

- Estrutura de sistema de informação (hardware e software). Segundo Economy, Powers e Jablonski (2015) é necessário assegurar o desenho da segurança cibernética dos elementos que suportam os processos da organização. Exigência de compra (hardware e software) de sistemas padronizados. Funcionalidade e fiabilidade dos sistemas de tecnologia da informação e comunicações. Aumentar o nível de demanda para compra de equipamentos sem dividir a parte funcional da segurança do produto.

- Desenvolvimento de exercícios e modelos de simulação. Analisando os autores Carayannis e Campbell (2015) a simulação é necessária para verificar o nível de resiliência cibernético do sistema, a eficácia das medidas tomadas, e a avaliação da velocidade de resposta, a realização de exercícios e modelos de simulação, tanto seja no interior como no exterior do sistema, é necessária.

- A atualização do quadro legal. Segundo o "*Tallinn Manual on the International Law Appicable to Cyber Warfare*" (2011) é necessário harmonizar a legislação do ambiente cooperativo de políticas de segurança de rede e informações, bem como o estabelecimento de autoridades nacionais para a coordenação e ativação de CERT.

- Cooperação privada, estadual, nacional e regional. Richards (2014) desenvolve o conceito que a cooperação entre as autoridades e agências de corpos de segurança e defesa é fundamental. Promover a cooperação e o intercâmbio de informações entre a indústria e os serviços de segurança cibernética.

- Ferramentas de desenvolvimento e melhoria contínua da segurança cibernética. Segundo Relia (2015) é importante levar em consideração as ferramentas de desenvolvimento e melhoria militares, de inteligência e de aqueles que suportam sistemas de comunicação estrategicamente importantes. Este último, em cooperação com os operadores privados. Para este tipo de ferramentas é desejável que a produção nacional tanto seja para gerar o *know-*

how de conhecimento, bem como para aperfeiçoar a blindagem no quadro local.

- A proteção física do patrimônio tecnológico. Donaldson et al. (2014) consideram que os sistemas de infraestruturas empregadas em segurança cibernética representam um ponto extremamente vulnerável como portas de entrada para o sistema ou como peças necessárias para o funcionamento harmonioso. A proteção física de tal patrimônio tecnológico também é essencial para alcançar a resistência desejada.

- Formação e especialização de capital humano. Segundo Hough et al. (2015), é necessária a formação contínua e permanente de capital humano para adquirir a experiência necessária para a tarefa. Ambiente profissional qualificado e com níveis extremos de conhecimento sobre as diferentes capas de segurança.

- Implantação e atualização das estratégias de resiliência cibernética (ciclo de vida). Estrada (2017) considera que essas estratégias devem ser aplicadas à segurança de rede, nós e áreas, formando uma defesa cibernética em profundidade e altura. Planos de gestão de segmentação e serviços de rede. Estratégias tais como seguir e prosseguir ou proteger e proceder. Ou seja, todo o procedimento e as ações apropriadas para a implantação que salvaguarde e permitirá que a organização possa retornar a um estado operacional no menor tempo possível. Então, será necessário adaptar todo o conjunto de medidas que estão disponíveis para a organização em intervalos apropriados (ciclo de vida).

- Dotação orçamental suficiente. Em referência com essa condição, a maioria da bibliografia consultada reforça a necessidade de contar com o orçamento adequado para a renovação e atualização de recursos humanos e materiais de forma contínua para garantir a resiliência dos sistemas cibernéticos.

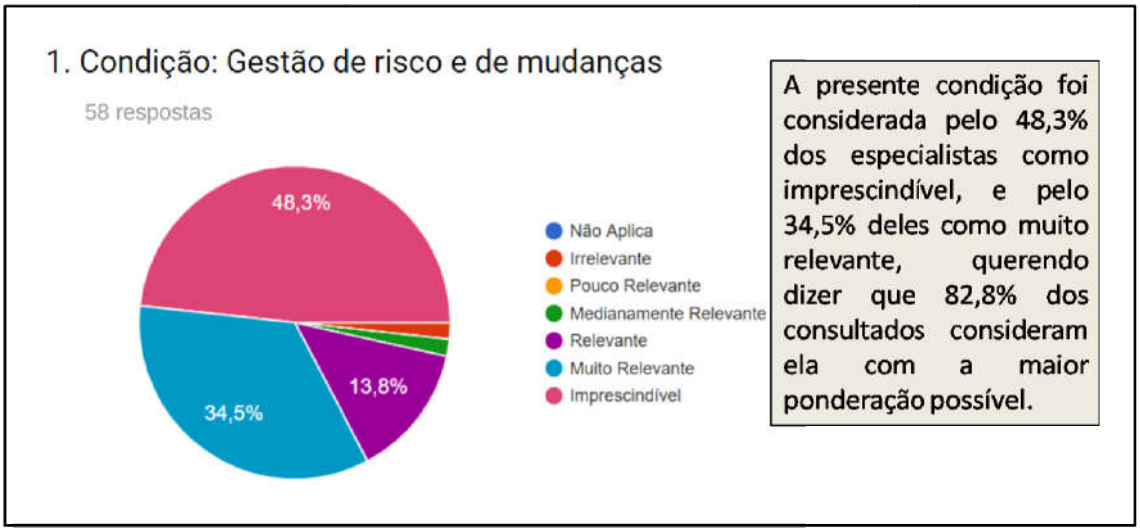
Todos esses condicionantes devem ser avaliados por especialistas no campo cibernético para definir qual seria um modelo de resiliência cibernética eficiente para ser implantado.

3. PROCURANDO UM MODELO DE RESILIÊNCIA CIBERNÉTICA

Tendo em vista os condicionantes elencados anteriormente, e com a intenção de consolidar um modelo de resiliência cibernética a partir da avaliação de especialistas destacados na área da cibernética (58 em total, pertencentes aos seguintes países: Argentina, Brasil, Chile, China, Colômbia, El Salvador, Equador, Espanha, Estados Unidos de América, Guatemala, México, Paraguai, Peru, Uruguai), feita por meio de um questionário de pesquisa (**APÊNDICE D – Especialistas consultados**), se pretende explorar os resultados obtidos extraindo conclusões de validade que permitam estabelecer o mecanismo causal entre as condições apresentadas no capítulo anterior e as surgidas a partir da visão dos especialistas concluindo com a proposta de um modelo mais aprimorado de resiliência cibernética.

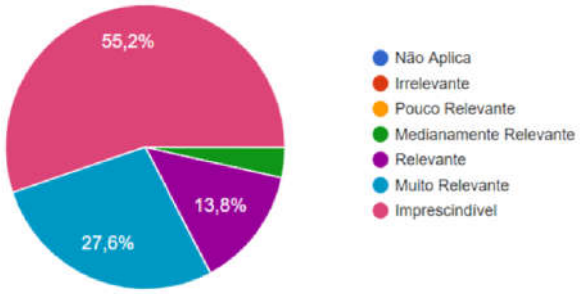
A seguir serão apresentados os resultados quantitativos da avaliação realizada pelos especialistas, discriminando cada condição identificada como possível componente de um modelo de ciber-resiliência e sua respectiva valoração considerando as variáveis em função de um peso maior em ordem de 7 (imprescindível) e menor em ordem de 1 (não aplica).

GRÁFICO 8–Resultados quantitativos dos questionários aos especialistas



2. Condição: Conhecimento profundo da organização (interna e externamente).

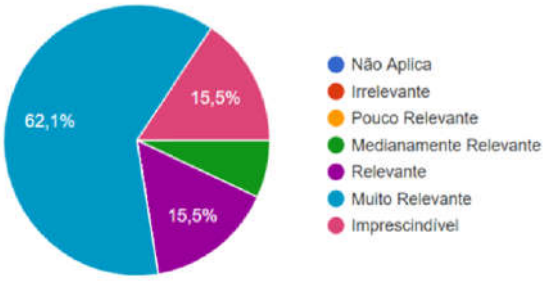
58 respostas



A presente condição foi considerada pelo 55,2% dos especialistas como imprescindível, e pelo 27,6% deles como muito relevante, querendo dizer que 82,8% dos consultados consideram ela com a maior ponderação possível.

3. Condição: Capacidade e participação no nível da organização de gerenciamento de tomada de decisão

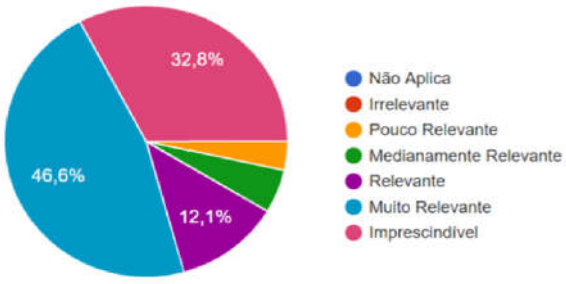
58 respostas



A presente condição foi considerada pelo 62,1% dos especialistas como muito relevante, pelo 15,5 % como imprescindível e pelo 15,5% como relevante, querendo dizer que seu nível de aceitação é de simples relevância, se posicionando em um nível de ponderação secundário.

4. Condição: Capacidade de antecipar a crise (CERT)

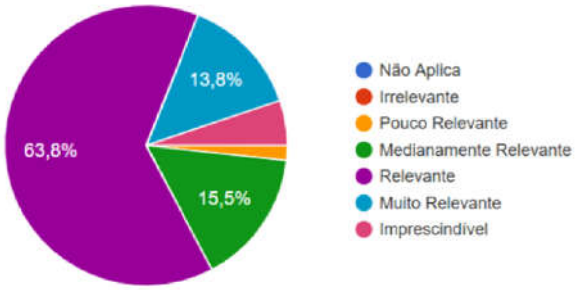
58 respostas



A presente condição foi considerada pelo 46,6% dos especialistas como muito relevante, pelo 32,8% como imprescindível, e pelo 12,1% como relevante, querendo dizer seu nível de aceitação é de relevância, se posicionando em um nível de ponderação positivo mais não imprescindível.

5. Condição: Simplificação de sistemas de informação para reduzir processos e interfaces

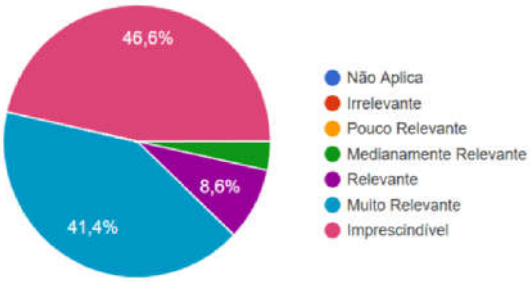
58 respostas



A presente condição foi considerada pelo 63,8% dos especialistas como relevante, pelo 15,5% deles como medianamente relevante, e só 13,8% como muito relevante, querendo dizer que seu nível de aceitação é de simples relevância, se posicionando em um nível de ponderação secundário.

6. Condição: Processos contínuos e operacionais em qualquer circunstância

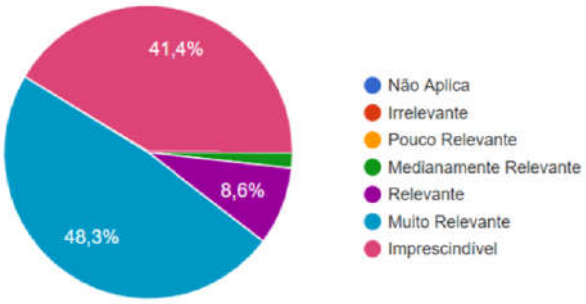
58 respostas



A presente condição foi considerada pelo 46,6% dos especialistas como imprescindível, e pelo 41,4% deles como muito relevante, querendo dizer que 88% dos consultados consideram ela com a maior ponderação possível.

7. Condição: Garantir regulamentos nas infra-estruturas críticas

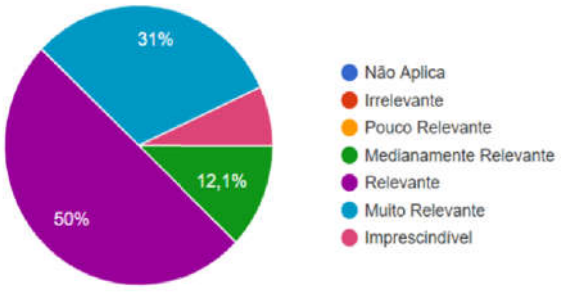
58 respostas



A presente condição foi considerada pelo 41,4% dos especialistas como imprescindível, e pelo 48,3% deles como muito relevante, querendo dizer que 89,7% dos consultados consideram ela com a maior ponderação possível.

8. Condição: Estrutura de sistema de informação (hardware e software)

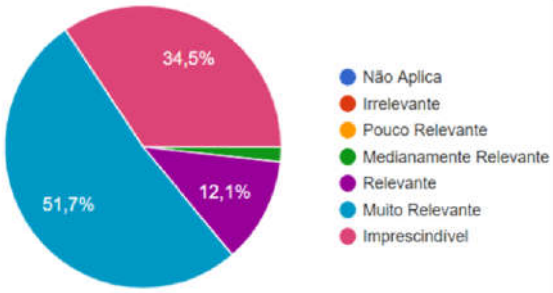
58 respostas



A presente condição foi considerada pelo 50% dos especialistas como relevante, pelo 31 % como muito relevante, e pelo 12,1% como medianamente relevante, querendo dizer que seu nível de aceitação é de simples relevância, se posicionando em um nível de ponderação secundário.

9. Condição: Desenvolvimento de exercícios e modelos de simulação

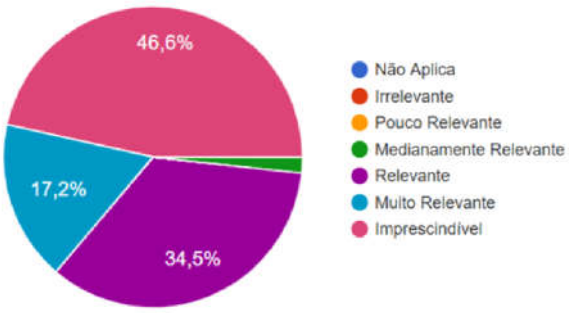
58 respostas



A presente condição foi considerada pelo 34,5% dos especialistas como imprescindível, e pelo 51,7% deles como muito relevante, querendo dizer que 86,2% dos consultados consideram ela com a maior ponderação possível.

10. Condição: A atualização do quadro legal

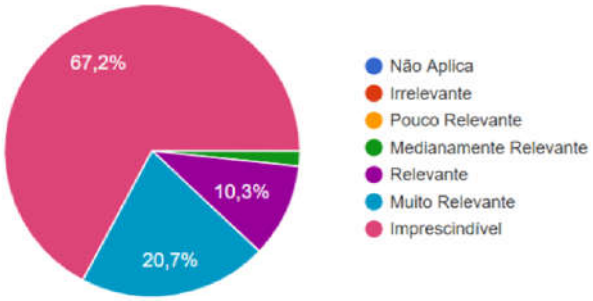
58 respostas



A presente condição foi considerada pelo 46,6% dos especialistas como imprescindível, pelo 17,2% como muito relevante, e pelo 34,5% deles como relevante, querendo dizer que seu nível de aceitação é de simples relevância, se posicionando em um nível de ponderação secundário.

11. Condição: Cooperação privada, estadual, nacional e regional.

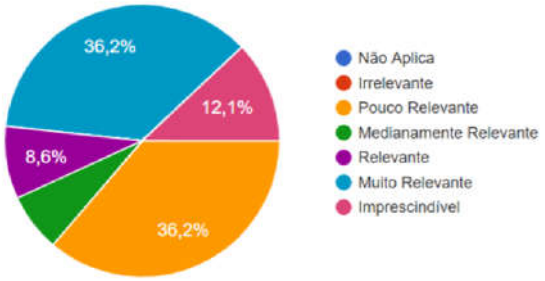
58 respostas



A presente condição foi considerada pelo 67,2% dos especialistas como imprescindível, e pelo 20,7% deles como muito relevante, querendo dizer que 87,9% dos consultados consideram ela com a maior ponderação possível.

12. Condição: Ferramentas de desenvolvimento e melhoria contínua da segurança cibernética

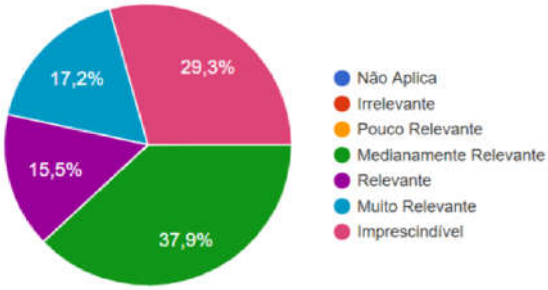
58 respostas



A presente condição foi considerada pelo 36,2% dos especialistas como pouco relevante, e pelo 36,2% deles como relevante, querendo dizer que seu nível de ponderação está muito por debaixo do pretendido para que seja uma condição necessária.

13. Condição: A proteção física do patrimônio tecnológico.

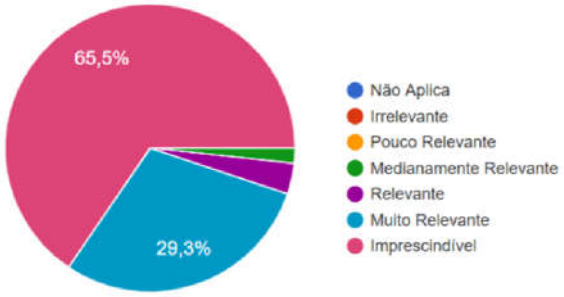
58 respostas



A presente condição foi considerada pelo 37,9% dos especialistas como pouco relevante, pelo 29,3% como imprescindível, e pelo 15,5% como relevante, querendo dizer que seu nível de ponderação está muito por debaixo do pretendido para que seja uma condição necessária.

14. Condição: Formação e especialização de capital humano.

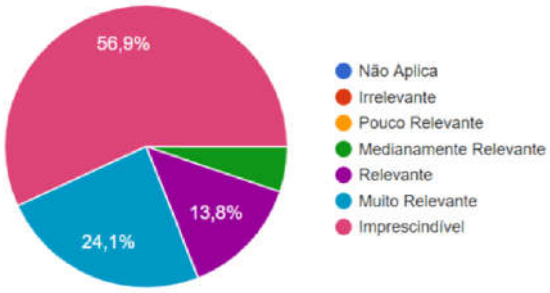
58 respostas



A presente condição foi considerada pelo 65,5% dos especialistas como imprescindível, e pelo 29,3% deles como muito relevante, querendo dizer que 94,8% dos consultados consideram ela com a maior ponderação possível.

15. Condição: Implantação e atualização das estratégias de ciber-resiliência (ciclo de vida)

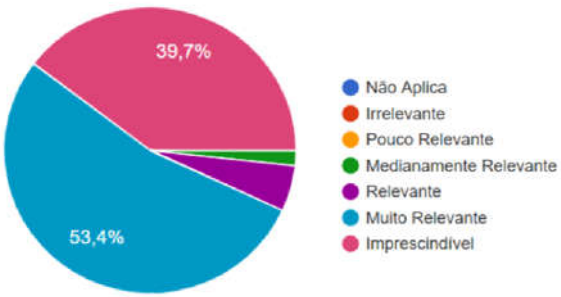
58 respostas



A presente condição foi considerada pelo 56,9% dos especialistas como imprescindível, e pelo 24,1% deles como muito relevante, querendo dizer que 81% dos consultados consideram ela com a maior ponderação possível.

16. Condição: Dotação orçamental suficiente.

58 respostas



A presente condição foi considerada pelo 39,7% dos especialistas como imprescindível, e pelo 53,4% deles como muito relevante, querendo dizer que 93,1% dos consultados consideram ela com a maior ponderação possível.

Fonte – O Autor.

Para uma melhor análise e visualização dos resultados das opiniões dos especialistas no que refere aos aspectos ponderados quantitativamente, se apresenta a seguir um quadro que condensa os resultados totais dos questionários.

QUADRO 2 – Quadro de síntese de resultados dos questionários dos especialistas.

Condição / Assunto	
Condição 1	**Gestão de risco e de mudanças**
Condição 2	**Conhecimento profundo da organização (interna e externamente)**
Condição 3	**Capacidade e participação no nível da organização de gerenciamento de tomada de decisão**
Condição 4	**Capacidade de antecipar a crise (CERT)**
Condição 5	**Simplificação de sistemas de informação para reduzir processos e interfaces**
Condição 6	**Processos contínuos e operacionais em qualquer circunstância**
Condição 7	**Garantir regulamentos nas infra-estruturas críticas**
Condição 8	**Estrutura de sistema de informação (hardware e software)**
Condição 9	**Desenvolvimento de exercícios e modelos de simulação**
Condição 10	**A atualização do quadro legal**
Condição 11	**Cooperação privada, estadual, nacional e regional**
Condição 12	**Ferramentas de desenvolvimento e melhoria contínua da segurança cibernética**
Condição 13	**A proteção física do patrimônio tecnológico**
Condição 14	**Formação e especialização de capital humano**
Condição 15	**Implantação e atualização das estratégias de resiliência cibernética (ciclo de vida)**
Condição 16	**Dotação orçamental suficiente**

Condição / Assunto	Porcentagens e Ponderação														TOTAL
	Imprescin-dível (%)	Coef 7	Muito Relevante (%)	Coef 6	Relevan-te (%)	Coef 5	Mediana-mente Relevante (%)	Coef 4	Pouco Relevante (%)	Coef 3	Irrele-vante (%)	Coef 2	Não aplica (%)	Coef 1	
Condição 1	48,3	338,1	34,5	207	13,8	69	1,7	6,8	0	0	1,7	3,4	0	0	624,3
Condição 2	55,2	386,4	27,6	165,6	13,8	69	3,4	13,6	0	0	0	0	0	0	634,6
Condição 3	15,5	108,5	62,1	372,6	15,5	77,5	6,9	27,6	0	0	0	0	0	0	586,2
Condição 4	32,8	229,6	46,6	279,6	12,1	60,5	5,2	20,8	3,4	10,2	0	0	0	0	600,7
Condição 5	5,2	36,4	13,8	82,8	63,8	319	15,5	62	1,7	5,1	0	0	0	0	505,3
Condição 6	46,6	326,2	41,4	248,4	8,6	43	3,4	13,6	0	0	0	0	0	0	631,2
Condição 7	41,4	289,8	48,3	289,8	8,6	43	1,7	6,8	0	0	0	0	0	0	629,4
Condição 8	6,9	48,3	31	186	50	250	12,1	48,4	0	0	0	0	0	0	532,7
Condição 9	34,5	241,5	51,7	310,2	12,1	60,5	1,7	6,8	0	0	0	0	0	0	619
Condição 10	46,6	326,2	17,2	103,2	34,5	172,5	1,7	6,8	0	0	0	0	0	0	608,7
Condição 11	67,2	470,4	20,7	124,2	10,3	51,5	1,7	6,8	0	0	0	0	0	0	652,9
Condição 12	12,1	84,7	36,2	217,2	8,6	43	6,9	27,6	36,2	108,6	0	0	0	0	481,1
Condição 13	29,3	205,1	17,2	103,2	15,5	77,5	37,9	151,6	0	0	0	0	0	0	537,4
Condição 14	65,5	458,5	29,3	175,8	3,4	17	1,7	6,8	0	0	0	0	0	0	658,1
Condição 15	56,9	398,3	24,1	144,6	13,8	69	5,2	20,8	0	0	0	0	0	0	632,7
Condição 16	39,7	277,9	53,4	320,4	5,2	26	1,7	6,8	0	0	0	0	0	0	631,1

Fonte – O Autor.

O raciocínio empregado para a elaboração do Quadro 2 é o seguinte:

- Em cada coluna que responde às variáveis de qualificação foi colocada a porcentagem atribuída segundo os valores obtidos e apresentados como Gráfico 6.

- Foram aplicados coeficientes de 1 até 7 considerando a relevância que essa condição tem para a constituição do modelo. Assim, o de menor relevância (não aplica) recebeu o valor 1, e o de maior (imprescindível) recebeu o valor 7.

- Foram feitas as multiplicações dos valores porcentuais um por um dos 16 coeficientes supramencionadas, e na última coluna (Total) foram somados todos os produtos, obtendo-se o valor final de ponderação atribuído a cada uma das condições.

Com o objetivo de categorizar os valores obtidos, serão apresentados quatro níveis de relevância das condições causais resultantes:

- **Primeiro Nível**, que envolve as mais altas ponderações e, consequentemente, as condições que serão consideradas como “necessárias” para constituir um modelo de resiliência cibernética (MAHONEY, 2010). Os valores contidos nesse nível estarão entre 658,1 e 619, de forma que os seguintes componentes do sistema estão contidos nessa categoria:

  - ➔ Condição 1: Gestão de risco e de mudanças.
  - ➔ Condição 2: Conhecimento profundo da organização (interna e externamente).
  - ➔ Condição 6: Processos contínuos e operacionais em qualquer circunstância.
  - ➔ Condição 7: Garantir regulamentos nas infraestruturas críticas.
  - ➔ Condição 9: Desenvolvimento de exercícios e modelos de simulação.
  - ➔ Condição 11: Cooperação privada, estadual, nacional e regional.
  - ➔ Condição 14: Formação e especialização de capital humano.
  - ➔ Condição 15: Implantação e atualização das estratégias de resiliência cibernética (ciclo de vida).
  - ➔ Condição 16: Dotação orçamental suficiente.

- **Segundo Nível**, que envolve aquelas condições cujas ponderações, não sendo as maiores, representam uma relevância tal que não poderiam ser descartadas do modelo. Assim, farão parte como subcondição de alguma das condições elencadas como de primeiro nível. Os valores contidos nesse nível estarão entre 618 e 580, encontrando-se contidos nessa categoria os seguintes componentes:

- ➔ Condição 3: Área da Cibernética com capacidade e participação no nível da organização de gerenciamento de tomada de decisão.
- ➔ Condição 4: Capacidade de antecipar a crise (CERT).
- ➔ Condição 10: A atualização do quadro legal.

- **Terceiro Nível**, que envolve aquelas condições cujas ponderações não foram consideradas como muito relevante, mas que poderiam se articular para contribuir de alguma maneira com a constituição do modelo, não sendo elas nem suficientes nem necessárias como tais. Os valores contidos nesse nível estarão entre 579 e 530, encontrando-se contidos nessa categoria os seguintes componentes:

- ➔ Condição 8: Estrutura de sistema de informação (*hardware e software*).
- ➔ Condição 13: A proteção física do patrimônio tecnológico.

- **Quarto Nível**, que envolve aquelas condições que, pela baixa ponderação dada pelos especialistas, não atende como requisito de um modelo cibernético resiliente, causa pela qual serão descartados do processo. Os valores contidos nesse nível estarão entre 530 e 480, encontrando-se nessa categoria os seguintes componentes:

- ➔ Condição 5: Simplificação de sistemas de informação para reduzir processos e interfaces.
- ➔ Condição 12: Ferramentas de desenvolvimento e melhoria contínua da segurança cibernética.

Da análise supracitada é possível extrair uma classificação preliminar de condições, subcondições e componentes como se apresenta a seguir:

QUADRO 3 – Modelo preliminar de condições, subcondições e componentes necessários para que um sistema seja considerado como ciber-resiliente.

N°	Condição	Subcondição	Componente	Observações
1	Gestão de risco e de mudanças			--
	1. a	Capacidade de antecipar a crise (CERT)		Ex Condição 4
2	Conhecimento profundo da organização (interna e externamente)			--
	2. a	Área da Cibernética com capacidade e participação no nível da organização de gerenciamento de tomada de decisão		Ex Condição 3
3	Processos contínuos e operacionais em qualquer circunstância			Ex Condição 6
			- Estrutura de sistema de informação (hardware e software)	Ex Condição 8
			- A proteção física do patrimônio tecnológico	Ex Condição 13
4	Garantir regulamentos nas infraestruturas críticas			Ex Condição 7
5	Desenvolvimento de exercícios e modelos de simulação			Ex Condição 9
6	Cooperação privada, estadual, nacional e regional			Ex Condição 11
	6. a	A atualização do quadro legal		Ex Condição 10
7	Formação e especialização de capital humano			Ex Condição 14
8	Implantação e atualização das estratégias de resiliência cibernética (ciclo de vida)			Ex Condição 15
9	Dotação orçamental suficiente			Ex Condição 16

Fonte – O Autor.

Como outro aspecto constituinte da análise, e partindo de uma visão qualitativa, serão exploradas as respostas apresentadas pelos especialistas referentes às outras condições que seriam convenientes adiar, respeitando a gradação descrita, para a criação de um modelo ciber-resiliente, extraindo de maneira sintética aqueles aspectos mais relevantes e abordados com maior frequência pelos especialistas, contribuintes para o aperfeiçoamento do modelo. Assim, os assuntos ou condições mais relevantes que serão tidos em conta para o presente estudo são:

QUADRO 4 – Assuntos ou condições mais relevantes tidas em conta das contribuições dos especialistas.

Conceito Geral	Síntese das opiniões dos especialistas
Estabelecimento de padrões de desempenho, de controle, desafio e resposta	• Estabelecimento de atributos de qualidade baseados em Standards. • Estabelecimento de controles de segurança críticos e vistorias periódicas relativas à resiliência. • Avaliação dos sistemas por meio de indicadores, a partir de diagnósticos contínuos e métricas adequadas. • Automatização de respostas a ameaças.
Normalização de protocolos e sistemas nos níveis nacionais e regionais	• Estabelecimento de uma Estratégia Nacional de Cibernética que integre todos os componentes do estado que contribuam com a cooperação entre os setores públicos e privados. • Existência de um glossário comum padronizado de termos relacionados com a cibernética para favorecer a cooperação. • Padronização dos sistemas a nível Estado (infraestrutura, software, procedimentos e políticas associadas).
Administração do pessoa da área e consciência situacional na população	• Formação adequada em engenharia social em todos os níveis. • Conscientização da organização, de todos os níveis de tomada de decisão e da sociedade sobre a importância da cibernética. • Preparação do público, em diferentes níveis, para conviver com sistemas cibernéticos. • Fidelização do pessoal vinculado às áreas de defesa cibernética, segurança informática e sistemas. • Constituição de uma equipe multidisciplinar com as seguintes capacidades: inteligência, contra-inteligências, gestão de risco, estudos de segurança

	física e informática, programação, recrutamento, auditores.
Cooperação, confiança e integração nacional e regional, pública e privada	• Disponibilidade de uma plataforma comum para compartilhar dados e assinaturas digitais de agressões cibernéticas (centros tecnológicos unificados). • Redundância, segmentação da informação e cooperação. • Necessidade de criar um ambiente de confiança mútua entre as organizações orientadas à defesa cibernética.
Proteção de ativos críticos	• Adequada capacidade de rastreabilidade ante qualquer incidente de segurança cibernética. • Incentivo ao desenvolvimento seguro de software no setor de programação da organização. • Clara categorização e priorização dos ativos a proteger.

Fonte - O Autor.

Considerando a pertinência e com a intenção de consolidar as informações ministradas pelos especialistas, serão categorizados os assuntos apresentados anteriormente em subcondições e componentes do modelo, a partir da execução de um processo de síntese no maior grau de conclusão possível, da seguinte maneira:

QUADRO 5 – Categorização das opiniões dos especialistas.

Categoria	Síntese das condições
Subcondições	• Estabelecimento de atributos de qualidade baseados em Standards e indicadores, a partir de diagnósticos contínuos e métricas adequadas. • Estabelecimento de uma Estratégia Nacional de Cibernética. • Padronização dos sistemas a nível Estado (infraestrutura, software, procedimentos e políticas associadas). • Clara categorização e priorização dos ativos a proteger.

Componentes	• Estabelecimento de controles de segurança críticos e vistorias periódicas relativas à resiliência. • Incentivo ao desenvolvimento seguro de software no setor de programação da organização. • Formação adequada em engenharia social em todos os níveis e conscientização da organização, de todos os níveis de tomada de decisão e da sociedade sobre a importância da cibernética. • Disponibilidade de uma plataforma comum para compartilhar dados e assinaturas digitais de agressões cibernéticas (centros tecnológicos unificados). • Adequada capacidade de rastreabilidade ante qualquer incidente de segurança cibernética. • Existência de um glossário comum padronizado de termos relacionados com a cibernética para favorecer a cooperação. • Automatização de respostas a ameaças. • Redundância, segmentação da informação e cooperação. • Necessidade de criar um ambiente de confiança mútua entre as organizações orientadas à defesa cibernética. • Fidelização do pessoal vinculado às áreas de defesa cibernética, segurança informática e sistemas. • Constituição de equipes multidisciplinares com as seguintes capacidades: inteligência, contra-inteligências, gestão de risco, estudos de segurança física e informática, programação, recrutamento, auditoria.

Fonte - O Autor.

Finalmente, alimentando o sistema com as subcondições e componentes extraídos da experiência dos especialistas, o modelo de ciber-resiliência que se apresente é o seguinte:

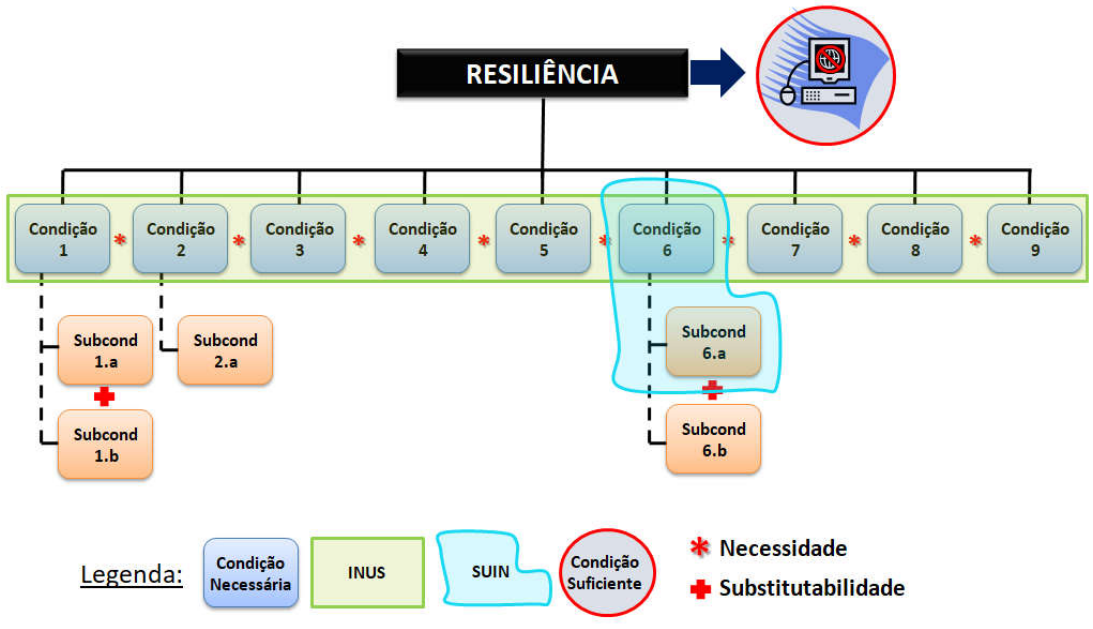
QUADRO 6 – Modelo final de condições, subcondições e componentes necessários para que um sistema seja considerado como ciber-resiliente.

N°	Condição	Sub-condição	Componente	Observações
1	Gestão de risco e de mudanças			--
		1. a	Capacidade de antecipar a crise (CERT)	Ex Condição 4
		1. b	Estabelecimento de atributos de qualidade baseados em standards e indicadores, a partir de diagnósticos contínuos e métricas adequadas	Especialistas
			- Adequada capacidade de rastreabilidade ante qualquer incidente de segurança cibernética.	Especialistas
			- Automatização de respostas a ameaças	Especialistas
2	Conhecimento profundo da organização (interna e externamente)			--
		2. a	Área da Cibernética com capacidade e participação no nível da organização de gerenciamento de tomada de decisão	Ex Condição 3
			- Formação adequada em engenharia social em todos os níveis e conscientização da organização, de todos os níveis de tomada de decisão e da sociedade sobre a importância da cibernética	Especialistas
3	Processos contínuos e operacionais em qualquer circunstância			Ex Condição 6
			- Estrutura de sistema de informação (hardware e software)	Ex Condição 8
			- A proteção física do patrimônio tecnológico	Ex Condição 13
			- Incentivo ao desenvolvimento seguro de software no setor de programação da organização	Especialistas
			- Estabelecimento de controles de segurança críticos e vistorias periódicas relativas à resiliência.	Especialistas
			- Redundância, segmentação da informação e cooperação.	Especialistas
4	Garantir regulamentos nas infraestruturas críticas			Ex Condição 7
			- Padronização dos sistemas a nível Estado (infraestrutura, software, procedimentos e políticas associadas)	Especialistas
			- Clara categorização e priorização dos ativos a proteger	Especialistas
5	Desenvolvimento de exercícios e modelos de simulação			Ex Condição 9

N°	Condição	Sub-condição	Componente	Observações
6	Cooperação privada, estadual, nacional e regional			Ex Condição 11
	6. a	A atualização do quadro legal		Ex Condição 10
	6. b	Estabelecimento de uma Estratégia Nacional de Cibernética		Especialistas
			- Existência de um glossário comum padronizado de termos relacionados com a cibernética para favorecer a cooperação	Especialistas
			- Necessidade de criar um ambiente de confiança mútua entre as organizações orientadas à defesa cibernética.	Especialistas
7	Formação e especialização de capital humano			Ex Condição 14
			- Fidelização do pessoal vinculado às áreas de defesa cibernética, segurança informática e sistemas.	Especialistas
			- Constituição de equipes multidisciplinares	Especialistas
8	Implantação e atualização das estratégias de resiliência cibernética (ciclo de vida)			Ex Condição 15
			- Disponibilidade de uma plataforma comum para compartilhar dados e assinaturas digitais de agressões cibernética	Especialistas
9	Dotação orçamental suficiente			Ex Condição 16

Fonte – O Autor.

GRÁFICO 9 – Esquematização das condições causais obtidas do processo de análise de evidências.



RESILIÊNCIA = (Cond 1 *Cond 2 * Cond 3 * Cond 4 * Cond 5 * Cond 6 * Cond 7 * Cond 8 * Cond 9)

Fonte – O Autor.

No gráfico supracitado, elaborado à luz do Mahoney (2010), é possível identificar como as 9 variáveis consideradas como principais constituem cada uma delas uma condição **necessária**, já que a resiliência não poderia ser obtida na ausência de alguma delas, mas também com sua presença individual, não basta para garantir o resultado.

Nesse mesmo raciocínio, poderia se aplicar a fórmula "RESILIÊNCIA = (Cond 1 *Cond 2 * Cond 3 * Cond 4 * Cond 5 * Cond 6 * Cond 7 * Cond 8 * Cond 9)" sendo o vetor " * " um vínculo de necessidade (ou seja que não podem estar ausentes essas condições da equação) para determinar que esse conjunto de variáveis conectadas constitui uma condição **INUS**, já que poderia definir-se que é uma parte insuficiente, mas necessária, de uma condição que é ela mesma não necessária, mas suficiente para o resultado.

Descendo o nível para o tratamento das subcondições identificadas no modelo, é possível construir as seguintes fórmulas: "Cond 1 = Subcond 1.a + Subcond 1.b" e "Cond 6 = Subcond 6.a + Subcond 6.b", sendo o vetor " + " um vínculo de substitutabilidade (ou seja que uma das duas subcondições levantadas para cada variável pode ser substituída), dando lugar assim à constituição de condições **SUIN**, sendo que cada uma delas poderia ser identificada como uma causa que é parte suficiente, mas não necessária, de um fator que é insuficiente, mas necessário, para o resultado. Quer disser que, tomando como exemplo parte do modelo, para alcançar a condição necessária de "gestão de risco e de mudanças" (condição Nr 1), foram identificadas duas subcondições: "capacidade de antecipar a crise (CERT)" (subcondição 1.a) e "estabelecimento de atributos de qualidade baseados em *standards* e indicadores, a partir de diagnósticos contínuos e métricas adequadas" (subcondição 1.b). É possível que a subcondição 1.a não esteja presente, mas que a condição 1 seja alcançada, devendo sim estar presente a subcondição 1.b (princípio de substitutabilidade). Essa relação de variáveis é chamada de causa SUIN.

Finalmente, e só aos fins de identificar no modelo a última das variáveis levantadas na literatura, só poderia existir uma causa chamada de "**suficiente**" para alcançar a resiliência cibernética desejada, considerando um sistema absolutamente isolado da rede, do contato físico com dispositivos externos de qualquer tipo, de qualquer interferência virtual ou física, alcançando a categorização de "circuito fechado". Sendo que uma causa suficiente é aquela na qual sua presença garante a concretização ou consumação do resultado que se deseja explicar, ou seja, que a presença dessa condição significa a existência do resultado (resiliência), só poderia ser considerada possível no caso de estudo se o sistema estivesse absolutamente isolado, atentando essa condição com o desempenho eficiente daquele modelo, tornando-o inviável.

4. É POSSÍVEL UMA AMÉRICA DO SUL CIBER-RESILIENTE?

Para responder essa pergunta primeiramente é necessária a abordagem de dois conceitos cruciais, a Difusão de Políticas (*Policy Diffusion*) e Transferência de Políticas (*Policy Transfer*), sendo que a diferencia entre os dois pode ser até difícil de perceber, razão pela qual serão apresentadas inicialmente definições acadêmicas disponíveis dos termos para após isso detalhar um quadro comparativo que possibilite um melhor entendimento.

Iniciando com a difusão de políticas, Levi-Faur (2005) entende que é “o processo mediante o qual a adoção da inovação por membros de um sistema social é comunicado através de determinados canais no tempo, ativando os mecanismos que incrementam a probabilidade de adoção por outros membros que ainda não os têm adotado” (p. 23, tradução nossa).

Outra visão diferente é a que apresentam Jordana et al. (2009), autores que entendem a difusão de políticas como o processo onde a informação referente a novas políticas ou instituições é comunicada através de certos canais no tempo entre membros de um sistema social de uma maneira descoordenada, onde as primeiras adoções da inovação afetam as probabilidades da adoção por quem não o têm feito.

Weyland (2006), por sua parte, destaca que é relevante distinguir se a difusão de políticas se trata de um modelo ou de um princípio. O primeiro se refere à difusão de uma política ou programa específico e concreto que se replica. O segundo se refere à difusão de um princípio, uma diretriz que lidera as decisões até determinadas políticas.

Esses autores afirmam que os estudos sobre difusão de políticas públicas constituem uma perspectiva de análise consolidada que contribui à compreensão dos processos de disseminação de políticas que possam ocorrer no interior de um país, ou a nível regional e global.

Por sua vez, a transferência de políticas é amplamente entendida como um processo mediante o qual o conhecimento das políticas, disposições administrativas, instituições e ideias em um sistema político (passado ou presente) se utilizam no desenvolvimento de características similares em outro (BENSON, 2000).

Bennet e Howlett (1992) a definem como “o aumento geral das políticas de conhecimento” (p. 288, tradução nossa). O dilema que se apresenta nesta afirmação é que só os seres humanos podem gerar e assimilar o conhecimento. Como Sabatier e Jenkins-Smith (1993) expõem, a aprendizagem orientada requer não só a assimilação do conhecimento, mas também a utilização dele sobre políticas em outros lugares, o que significa no mínimo, levar em consideração o conhecimento de políticas em outros lugares. Essa transferência de políticas é usualmente utilizada pelos governos, sendo chamada de aprendizagem organizacional.

Argyris e Schon (1994) fazem uma abordagem à aprendizagem organizacional ao inferirem que, como “ela ocorre quando os homens atuam em nome da organização e interagem com outros”. Nesse caso, “a aprendizagem deriva das crenças, atitudes e valores desses membros relevantes da organização, e enquanto à transferência de políticas, o comportamento organizacional também muda” (p.191, tradução nossa).

Como foi visto, a diferencia entre esses dois conceitos não é simples de se identificar. É por isso que, a partir de uma análise aprofundada da literatura apresentada por Obingera, Shmitta e Stakea (2013), foi possível construir um

quadro comparativo entre a transferência e a difusão de políticas que permite entender mais pormenarizada esses conceitos.

QUADRO 1 – Comparação entra transferência e difusão de políticas.

Critérios	Transferência de Políticas	Difusão de Políticas
Definição	Processo que denota ações políticas que utilizam o conhecimento sobre políticas, disposições administrativas, instituições e ideias em um sistema político para o desenvolvimento de políticas, disposições administrativas, instituições e ideias de outro sistema político.	Processo pelo qual as decisões políticas em um país afetam as decisões políticas de outros países.
Orientação da literatura	Baseia-se no trabalho prévio em relação ao desenho.	Refere-se à literatura quantitativa sobre a difusão de inovações e adoção de programas.
Motivação	Relevância do conhecimento e o papel dos processos internacionais (agências).	Geralmente inclui processos estruturais, baseados em interesses.
Enfoque Metodológico	Dominante na pesquisa orientada os estudos de casos.	Utiliza-se com maior frequência na literatura de pesquisa quantitativa.
Propósito	Tanto a política de difusão quanto a transferência de políticas se referem às interdependências entre os sistemas políticos no processo de tomada de decisão.	
Finalidade	Descrever e explicar que as políticas são resultado de decisões interdependentes.	

Fonte: Adaptação do autor dos conceitos apresentados por Obingera, Shmitta e Stakea (2013)

Como informações adicionais relevantes os autores Obingera, Shmitta e Stakea (2013) afirmam que as diferencias entre os dois processos são marginais, sendo em sua maioria fundados na diferentes tradições de pesquisa, deixando claro que, no decorrer do tempo, é possível que existam crescentes similitudes nos resultados obtidos, aplicando um ou outro processo.

Baseado nesta última afirmação, e considerando que a presente pesquisa é de caráter qualitativa, que se orienta no mapeamento de um caso histórico, que se motiva na relevância do conhecimento e do papel dos processos internacionais, e que tem uma estreita relação com o desenho de um modelo, é que será abordada a literatura de transferência de políticas como ferramenta de referência.

A história demonstra que um modelo aplicável numa determinada região pode não dar certo em outra região, por diversas questões subjacentes, tanto endógenas como exógenas nesse ambiente. É por isso, que empregando a técnica de transferência de políticas, tomando como referência a Dolowitz e Marsh (2000), somado à revisão bibliográfica feita por Benson e Jordan (2011), se buscará transferir esse modelo à América do Sul, cuja realidade é suficientemente diferente a da Europa, para ser importada diretamente.

Abordando a problemática desde uma ordem cronológica, será apresentado a seguir a visão de Dolowitz e Marsh (2000) ao respeito da transferência de políticas. Esses autores afirmam esse processo se organiza em torno de seis perguntas, sintetizadas no quadro abaixo:

QUADRO 7 – Visão de Dolowitz e Marsh (2000) ao respeito da transferência de políticas

Pergunta [8]	**Orientação**

[8] DOLOWITZ, D. P.; MARSH, Y. D. Learning for abroad : The rule of policy transfer in the actual politics decitions. **Dolowitz y Marsh Revisited**. [S.l.]:v. 13, n. 1, p. 8, 2000.

Pergunta	Orientação
Por que atores participam na transferência de políticas?	Os atores participam na transferência de políticas voluntariamente, coercitivamente, ou misturando essas duas variantes. Voluntariamente a partir da modelagem das lições apreendidas, o que pressupõe uma racionalidade perfeita. Coercitivamente, a partir de uma imposição direta dada por grupos de pressão, partidos políticos, empresários ou especialistas em política. E Misturadamente a partir da modelagem das lições apreendidas a partir de uma racionalidade limitada, surgida por pressões internacionais (imagem, consenso, percepções), de condicionantes (empréstimos, condições associadas à atividade empresarial), e obrigações.
Quem são os atores chave envolvidos no processo de transferência de políticas?	Primeiramente é preciso reconhecer e distinguir entre os países que são normalmente prestamistas e os que são pelo geral os que recebem esses benefícios, sendo que essa relação deve evitar ser desproporcionada. Mesmo assim, isto não é uma regra universal. Às vezes países classificados como prestamistas extraem lições entanto os países classificados como beneficiários atuam como modelos para outros sistemas políticos. Assim, poderiam se classificar nove categorias principais de atores políticos envolvidos na transferência de políticas: os funcionários escolhidos;

	os partidos políticos; burocratas / funcionários; grupos de pressão; empresários; especialistas em políticas empreendedoras; corporações transnacionais; grupos de reflexão; organismos supra-institucionais, governamentais e não governamentais.
O quê se transfere?	Na atualidade quase qualquer coisa pode ser transferida de um sistema político a outro, dependendo do tema ou situação em questão. Mesmo assim, podem se distinguir oito categorias diferentes: objetivos da política, conteúdos da política, instrumentos da política, programas da política, instituições, ideologia, idéias e atitudes.
De onde se extraem lições?	Em essência, argumenta-se que os responsáveis políticos podem olhar aos três níveis de governo: internacional, nacional e local. Dentro de uma nação, os atores que participam na transferência de políticas podem aprender de outros sistemas políticos ou unidades do seu próprio país. Também é comum que os governos e os agentes transfiram as políticas de uma nação para outra. Além disto, é importante extrair as lições obtidas por outros países, não só olhar para governos nacionais, mas também olhar para outros níveis sub-nacionais e unidades de governo. Finalmente, as lições podem se extrair, forçados em um sistema político, do nível internacional.
Quais são os diferentes graus de transferência?	A transferência de políticas não é um processo de todo ou nada, já que qualquer caso em particular pode implicar a combinações. Mesmo assim, existem basicamente quatro gradações diferentes (ou graus de transferência): colar, que

	implica a transferência direta e completa; emulação, que implica a transferência das ideias detrás da política ou programa; combinações, que mistura várias políticas diferentes; e inspiração, onde a política em outra jurisdição pode inspirar um cambio
O que restringe o processo de transferência de políticas?	O processo pode ser restringido a partir da própria complexidade política; pelas diversas publicações que estejam disponíveis em jornais, revistas, TV ou rádio; pela estrutura; pelas próprias instituições; pela viabilidade (ideologia, proximidade cultural, tecnologia, economia, burocracia); e pela linguagem.
Como é o processo de transferência de políticas relacionado com a política do sucesso ou do fracasso?	Enquanto ao sucesso, a partir da demonstração dessa transferência por meio da mídia, relatórios, conferências, reuniões, visitas, declarações (escritas ou verbais). Como a transferência leva à falha de política. Enquanto ao fracasso, a transferência leva à falha da política a partir da transferência não uniformizada, transferência incompleta, transferência inadequada.

Fonte: Adaptação do autor dos conceitos apresentados por Dolowitz e Marsh (2000), tradução nossa.

Aprofundado ainda mais os conceitos apresentados, Benson e Jordan (2011) formulam-se uma série de perguntas para orientar o processo de revisão da literatura Dolowitz e Marsh (2000), oferecendo também as correspondentes respostas baseadas em diversas produções acadêmicas. Assim, poderiam se identificar os seguintes aspectos relevantes para a nossa pesquisa:

QUADRO 8 – Síntese de revisão acadêmica de Benson e Jordan (2011).

Pergunta	Orientação
Quais elementos da	Objetivos da política, estrutura e conteúdo;

política se transferem?	instrumentos da política ou técnicas administrativas; instruções; ideologias; idéias, atitudes e conceitos; lições negativas.
Existem diferentes tipos de transferência?	Inicialmente foram identificados: a colagem de termos, a emulação, a hibridação, a síntese e inspiração. Na atualidade pretende-se combinar a hibridação com a síntese para denotar os casos em que os elementos da política estão desenhados em base a diferentes contextos. Entretanto, na atualidade existem muitas mais categorias e tipos de transferência a considerar.
Desde onde se transferem essas políticas?	Originariamente a transferência de políticas se dava tanto de fonte endógenas quanto exógenas. Mas cada vez mais as pessoas que trabalham desde uma perspectiva de europeização, globalização, governança multilateral, a rede de políticas tem sugerido que as lições também podem ser extraídas e transferidas facilmente entre muitos outros lugares diferentes, que abarcam múltiplas escalas espaciais e temporais.
Quais fatores permitem e limitam essa transferência?	Dependência da trajetória que surge das decisões passadas; impedimentos institucionais e estruturais; falta de compatibilidade ideológica entre países de transferência; insuficientes recursos tecnológicos, econômicos, burocráticos e políticos para implementar as políticas de transferência.

Fonte: Adaptação do autor dos conceitos apresentados por Benson e Jordan (2011), tradução nossa.

Sintetizando as análises realizadas, apresentam-se a seguir os interrogantes (devidamente adaptados da literatura estudada), que serão tidos

em conta para a aplicação prática da teoria no contexto da transferência de políticas públicas da OTAN para a América do Sul:

- Por que se pretende que atores participem na transferência de políticas no âmbito da resiliência cibernética?
- Quem são os atores chave envolvidos no processo de transferência de políticas entre a OTAN e a América do Sul?
- O quê se pretende transferir e de onde foram extraídas as lições para seja feita?
- Quais são os diferentes graus de transferência e qual sua possível projeção no tempo?
- Quais fatores permitem e limitam o processo de transferência de políticas no caso particular da América do Sul?

Nas subsecções seguintes serão respondidas cada uma das perguntas levantadas, na mesma ordem apresentada, com a intenção de aplicar a teoria à realidade regional.

4.1 POR QUE SE PRETENDE QUE ATORES PARTICIPEM NA TRANSFERÊNCIA DE POLÍTICAS NO ÂMBITO DA RESILIÊNCIA CIBERNÉTICA?

Seguindo a classificação apresentada por Dolowitz e Marsh (2000), poderia se afirmar que os atores participam de uma transferência voluntária, que pressupões, a partir de uma racionalidade perfeita, a modelagem do modelo pretendido a partir das lições apreendidas, neste caso pela OTAN.

Assim, entende-se que atores participem na transferência porque a estrutura organizacional da OTAN em matéria de ciberdefesa e cibersegurança encontra-se solidamente desenvolvida a partir da constituição do Centro de Excelência Cooperativo de Ciber Defesa e a implementação de medidas de desempenho padronizadas que possibilitam o crescimento na matéria,

sustentando a confiança mútua entre os países que integram essa aliança, e robustecendo os sistemas cibernéticos neles contidos.

Em contrapartida, a América do Sul não tem estruturas muito incipientes nessa matéria. Mesmo sendo a OEA um organismo tão antigo quanto a OTAN, as atividades de cooperação e integração na área da cibernética são recentes, e não há nenhum órgão semelhante ao CECCD, re-lembrando que aqueles dois princípios mencionados (cooperação e integração) são essenciais para que a resiliência possa ser viável.

4.2 QUEM SÃO OS ATORES CHAVE ENVOLVIDOS NO PROCESSO DE TRANSFERÊNCIA DE POLÍTICAS ENTRE A OTAN E A AMÉRICA DO SUL?

Segundo o apresentado por Dolowitz e Marsh (2000), pode se identificar à OTAN como prestamista do modelo, fundamentando isto com todos aqueles argumentos já desenvolvidos antecipadamente. O problema que se apresenta agora é qual será o organismo na América do Sul que possa se identificar como beneficiário, considerando, segundo a classificação sugerida por esses autores, que seria um organismo supra-institucional equivalente à OTAN, mas na região.

Para atender a realidade regional, na América do Sul, podem se distinguir três atores bem diferenciados, os quais serão analisados, para se extrair um deles como o mais adequado para simular a transferência. Esses atores são:

- OEA (Organização de Estados Americanos);
- UNASUL (União de Nações Sul-Americanas);
- PROSUL (Foro para o Progresso Sul-Americano).

A OEA é uma organização fundada em 1948, com sede em Washington – Estados Unidos da América, que tem por finalidade construir uma ordem de paz e de justiça no continente americano, promover a solidariedade, o desenvolvimento e a cooperação entre os Estados da Região, além de defender a democracia e os direitos humanos (BRASIL, 2019).

Tem funções essencialmente diplomáticas e representativas, já que se trata de um foro de cooperação política. Mesmo assim, está facultada a exercer certo nível de coerção, caso seja necessário, sempre que não vulnere os princípios fundamentais da sua carta constitutiva, como o direito à soberania das nações e sempre que tenha o voto positivo dos Estados membros (OEA, 2019).

Mejias (2008) descreve que a Organização de Estados Americanos está composta pelos seguintes países: Argentina, Bolívia, Brasil, Chile, Colômbia, Costa Rica, Cuba, República Dominicana, Equador, El Salvador, Estados Unidos, Guatemala, Haiti, Honduras, México, República Dominicana, São Cristóvão e Neves, Nicarágua, Panamá, Paraguai, Peru, Uruguai, Barbados, Trindade e Tobago, Jamaica, Granada, Suriname, Canadá, Guiana, Belize, Bahamas, São Vicente e Granadinas, Antiga e Barbuda, Santa Lúcia, Venezuela (país que se encontra em processo de separação).

A UNASUL é uma organização que nasceu em Brasília, em 2008, sendo integrada na sua constituição por doze países da América do Sul: Argentina, Bolívia, Chile, Colômbia, Equador, Guiana, Paraguai, Peru, Suriname, Uruguai e Venezuela (UNASUR, 2011).

Nasceu com o objetivo de construir um espaço de integração e união social, econômica, cultural e política entre os países sul-americanos.

Na atualidade, encontra-se em um processo de dissolução por diversas causas de ordem política e organizacional, abandonando a dita organização os seguintes países: Peru, Colômbia, Argentina, Chile, Brasil, Equador e Paraguai; só ficando ainda na sua estrutura Bolívia, Guiana, Suriname, Uruguai e Venezuela (SABATINI e ALBARTONI, 2019).

O primeiro país ao se afastar da UNASUR foi a Colômbia, em agosto de 2018 e já em janeiro de 2019, o Presidente desse país (Iván Duque) anunciava a intenção de diversos governos ibero-americanos em criar uma organização, a qual chamariam de PROSUR. Essa intenção foi apoiada de maneira imediata pelo presidente do Chile, Sabastián Piñeira, que assinalou que esse novo foro estaria aberto para todos os países da América do Sul que respeitem o pleno Estado de Direito e promovam o respeito das liberdades e dos direitos humanos (SABATINI e ALBARTONI, 2019).

O PROSUR começou funcionar em 22 de março de 2019, quando foi executada a primeira reunião dessa organização, que teve lugar em Santiago de Chile, aonde participaram os seguintes países: Argentina, Brasil, Chile, Colômbia, Equador, Paraguai e Peru. Como observadores, mas não membros do Foro, nem assinantes do protocolo, estiveram presentes também: Bolívia, Suriname e Uruguai (SABATINI e ALBARTONI, 2019).

No dia 23 de julho de 2019, foi feita a primeira reunião de Coordenadores Nacionais do PROSUR, em Santiago do Chile, sede da Presidência pro-tempore da dita organização. Nesse evento, o Ministro das Relações Exteriores do Chile (Teodoro Ribera) manifestou que os países participantes compartilham a intenção estratégica de que a região seja reconhecida no cenário global. Nessa reunião, foram abordadas como áreas de prioridade do Foro, as seguintes: infraestrutura, energia, saúde, defesa, segurança e combate ao crime, preservação e manejo de desastres naturais (CHILE, 2019).

Segundo o apresentado até agora, e considerando que a América do Sul possui de organização em processo de dissolução (UNASUL) e outra em processo de criação (PROSUL), sem uma estrutura definida ainda, é a OEA a que certamente atende com maior abrangência os esforços cooperativos e de integração da América do Sul.

A partir de um processo exploratório dos principais portais da OEA, organizações relacionadas e organismos governamentais dos países da região, serão elencados, a seguir, uma série de notícias e informações que permitirão extrair conclusões sobre a relevância ou não da OEA como ator regional facilitador da articulação do modelo de resiliência cibernética apresentado.

Os critérios empregados para a seleção desses portais de notícias foram: tomar como data de início da pesquisa o início do processo de dissolução da UNASUL, a partir da declaração da Colômbia de se afastar dessa organização em agosto de 2018; e que esses portais sejam oficiais ou forneçam informações oficial dos governos da região.

QUADRO 9 – Síntese de notícias oficiais sobre a participação da OEA na área da cibernética.

Data	País / Região	Notícia
03/08/2018	Argentina	A Diretoria Nacional de Cooperação Internacional da Segurança do Ministério de Segurança da República Argentina, em conjunto com a Diretoria Nacional de Inteligência Criminal, receberam a capacitação internacional sobre Cibersegurança, dentro de um programa de Liderança e Estratégia de Cibersegurança. A organização do programa coube à Organização de Estados Americanos e à *Florida International University*. Dessa maneira, continuam se consolidado ações de cooperação internacional, tendo em vistas os desafios contemporâneos que apresentam as ameaças cibernéticas e sua projeção futura. Com o objetivo de atualizar informações para prevenir riscos em matéria de cibersegurança, o programa incluiu módulos sobre ameaças cibernéticas, estratégias operacionais da segurança, assuntos nacionais em matéria de segurança cibernética e exercícios de simulação de respostas (ARGENTINA, 2018).
23/09/2018	América Latina e Caribe	A OEA apresenta um Relatório sobre Cibersegurança e Entidades Bancárias em América Latina e o Caribe, no âmbito o Simpósio de Cibersegurança oferecido pela própria organização. Esse informe realiza uma análise exaustiva do estado das entidades bancárias da região em relação a diferentes aspectos de segurança cibernética. 92 % das entidades bancárias da América Latina foram vítimas de algum incidente cibernético no último ano e 37 % delas sofreram ataques com resultados bem-sucedidos por parte dos criminosos (OEA, 2018).

Data	País / Região	Notícia
24/10/2018	América	A Secretaria Geral da OEA e Amazon Web Services (AWS) apresentaram na Colômbia um Livro Branco conjunto que aborda os desafios e oportunidades que a cibersegurança envolve nas cidades, e estabelece recomendações para a sustentabilidade das cidades inteligentes. Esse documento é o quarto de uma serie que, junto a outras iniciativas conjuntas, procura aumentar o nível de consciência dos líderes governamentais, o setor privado e a sociedade em geral sobre a importância da cibersegurança (OEA, 2018).
28/11/2018	América	A Junta Interamericana de Defesa, por delegação da OEA, realizou uma Conferência de Ciberdefesa com a finalidade de propor recomendações aos Estados Membros da OEA sobre a segurança no manejo de informações através do ciberespaço e a proteção dos meios informáticos. Essa foi a primeira conferência em Cibersegurança no Hemisfério intitulada “Ciberdefesa nas Américas: Importância do Ciberespaço como Campo de Batalha do Século XXI“, cujo propósito foi apresentar um panorama geral da importância na aplicação de diversas medidas de segurança no manejo da informação ante os riscos de sofrer um ataque cibernético. Tal conferência contou com a presença diferenciada do Coronel do Exército Brasileiro João Carneiro, especialista em ciberdefesa, que contribuiu com a elaboração do presente estudo (através do questionário de pesquisa).

Data	País / Região	Notícia
14/12/2018	Paraguai	Apresentação do Plano Nacional de Cibersegurança do Paraguai. Participaram dessa apresentação diversos setores envolvidos no tema da cibersegurança do Paraguai sobre o apoio e facilitação da OEA (PARAGUAI, 2018).
06/03/2019	Chile e América	Simpósio de Cibersegurança da OEA 2019, que será feito entre os dias 24 e 27 de setembro de 2019 na cidade de Santiago de Chile. O Chile assume a Presidência do Grupo sobre medidas de fomento da confiança e cooperação no ciberespaço da OEA. Na reunião desse grupo, realizada em abril de 2019, contou-se com a participação de representantes dos países da região, especialistas internacionais, junto com o apoio e auspicio da Secretaria Executiva do Comitê Internacional contra o Terrorismo da OEA (CHILE, 2019).

Fonte: O Autor.

A intenção de apresentar as notícias supracitadas foi simplesmente para demonstrar a relevância que a OEA está tendo no âmbito da América do Sul em matéria de defesa e segurança cibernética, pudendo ser então considerada como organização homóloga à OTAN para exercitar o processo de transferência de políticas públicas para a aplicação ou não do modelo criado.

Além disto, e para reforçar a postura adotada, serão apresentadas a seguir uma série de opiniões dos especialistas consultados nos respectivos questionários (GÓMEZ, 2019) sobre a possibilidade ou não da transferência das experiências da OTAN para a América do Sul, surgiu um consenso bastante amplo ao respeito de que a OEA seja o órgão regional responsável de fazer o sistema de cooperação e integração funcionar.

Em síntese, uma ampla maioria desses especialistas considera que é possível a transferência a partir da cooperação atualmente existente com a OEA, revalidando o apresentado anteriormente. Mesmo assim, é necessária a obtenção de unificação de critérios, criando e fortalecendo um marco cooperativo sobre a base da confiança mutua.

Também foi apresentada como problemático o vazio legal existente, a falta de coerência ideológica entre países da região e a ausência de políticas de uma supra-estrutura organizacional regional que seja reconhecida de comum censo.

4.3 O QUÊ SE PRETENDE TRANSFERIR E DE ONDE FORAM EXTRAIDAS AS LIÇÕES PARA SEJA FEITA?

No critério dos autores Dolowitz e Marsh (2000), no presente caso de estudo, as categorias de políticas que poderiam ser transferidas seriam: objetivos, instrumentos, programas e atitudes, dirigindo seu olhar tanto ao âmbito internacional (inicialmente regional, sem se desconectar da realidade global), e nacional (considerando a particularidade que possui cada país-membro).

Ligado com o parágrafo supracitado, o que se pretende é transferir o Modelo de Resiliência Cibernética criado a partir das lições obtidas pelas boas práticas da OTAN na matéria, convenientemente exploradas ao longo do presente estudo, e pela visão dos quase 60 especialistas na área que contribuíram com a pesquisa.

Tal modelo proposto, que envolve objetivos, instrumentos, programas e atitudes a serem articuladas, poderia se sintetizar nos seguintes assuntos:

QUADRO 10 – Síntese de assuntos contidos no modelo a ser transferido.

Gestão de risco e de mudanças (adequada capacidade de rastreabilidade ante qualquer incidente de segurança cibernética e automatização de respostas a ameaças), amparado isto com uma adequada capacidade de antecipar a crise (CERT) e o estabelecimento de atributos de qualidade baseados em

Standards e indicadores, a partir de diagnósticos contínuos e métricas adequadas.
Conhecimento profundo da organização (formação adequada em engenharia social em todos os níveis e conscientização da organização, de todos os níveis de tomada de decisão e da sociedade sobre a importância da cibernética), o que traz como consequiência que a área da cibernética conte com capacidade e participação no nível da organização de gerenciamento de tomada de decisão.
Processos contínuos e operacionais em qualquer circunstância (estrutura de sistema de informação, proteção física do patrimônio tecnológico, incentivo ao desenvolvimento seguro de software no setor de programação da organização, estabelecimento de controles de segurança críticos e vistorias periódicas relativas à resiliência, redundância, segmentação da informação e cooperação).
Garantir regulamentos nas infraestruturas críticas (padronização dos sistemas a nível Estado e clara categorização e priorização dos ativos a proteger).
Desenvolvimento de exercícios e modelos de simulação.
Cooperação privada, estadual, nacional e regional (existência de um glossário comum padronizado de termos relacionados com a cibernética para favorecer a cooperação e necessidade de criar um ambiente de confiança mútua entre as organizações orientadas à defesa cibernética). Para isto, é precisa a atualização do quadro legal e o estabelecimento de uma Estratégia Nacional de Cibernética para cada estado-membro.
Formação e especialização de capital humano (fidelização do pessoal vinculado às áreas de defesa cibernética, segurança informática e sistemas e constituição de equipes multidisciplinares).
Implantação e atualização das estratégias de resiliência cibernética (disponibilidade de uma plataforma comum para compartilhar dados e assinaturas digitais de agressões cibernéticas).
Dotação orçamentária suficiente.

Fonte: O Autor.

4.4 QUAIS SÃO OS DIFERENTES GRAUS DE TRANSFERÊNCIA E QUAL SUA POSSÍVEL PROJEÇÃO NO TEMPO?

Sendo as gradações propostas por Dolowitz e Marsh (2000) colar, emular, combinar ou inspirar, o que se pretende é aplicar uma combinação para fazer possível dita transferência. Mesmo assim, e para o caso particular de estudo, foram propostas também gradações no processo de aplicação de dita transferência, como maneira de fazer mais plausível e viável sua implementação.

Assim, foram estabelecidos os seguintes graus de transferência (em profundidade), identificando um primeiro grau como imediato, um segundo como de curto e médio prazo, e um terceiro como de longo prazo.

QUADRO 11 – Graus de transferência para o modelo pretendido.

Grau	Medidas
1º Grau	Gestão de risco e de mudanças. Segundo foi apresentado, essas são medidas que na atualidade estão já sendo implementadas nos países da região, considerando a necessidade de preservação das próprias informações e sistemas.
	Desenvolvimento de exercícios e modelos de simulação. Esse é outro assunto que está sendo trabalhado de maneira bilateral e regional como um todo, por iniciativa de países como o Brasil, a Colômbia e o Chile, principalmente.
	Formação e especialização de capital humano. Alinhados com o raciocínio das duas condições anteriores, a formação e especialização do capital humano está sendo um assunto de extrema relevância.
2º Grau	Processos contínuos e operacionais em qualquer circunstância. Mesmo que estejam sendo trabalhadas e possam ser trazidas no primeiro grau de transferência à região as medidas de gestão de risco e de mudança, os processos contínuos e operacionais em qualquer circunstância requerem uma infraestrutura cooperativa e integrada na região que tem que ser construída, mas que não pode ser feita no curto prazo.

Grau	Medidas
2º Grau	Garantir regulamentação nas infraestruturas críticas. Mesmo sendo as infraestruturas críticas a responsabilidade de cada Estado protegê-las, sendo eles soberanos para fazê-lo ou não, a cooperação e integração regional ajudaria muito na padronização de medidas a serem adotadas para cada tipo de infraestrutura crítica, além daquelas que têm incidência além das fronteiras dos países. O tempo de maturidade, de adequação e implementação dessas medidas pode demorar um período que com certeza não será no curto prazo.
	Cooperação privada, estadual, nacional e regional. Essa condição faz parte do processo. Alguns países da região já estão encaminhados nesse caminho, mas regionalmente, ainda tem que ser trabalhado bastante, a cooperação e a integração regionais. Internamente, é possível que exista, mas regionalmente ainda é incipiente.
	Implantação e atualização das estratégias de resiliência cibernética. Da mesma maneira que foi feito na OTAN, com diretrizes e orientações para os países membros, poderia ser uma boa prática para que cada país da região adéque suas estratégias de cibersegurança e ciberdefesa, tendendo ao estabelecimento de padrões de desempenho comuns que favoreçam a sinergia e faça mais robusta a segurança regional.
3º Grau	Conhecimento profundo da organização. Foi colocado nesse grau de transferência porque ainda a região não tem definida uma organização internacional que coordene e regule o espaço cibernético, mesmo que seja só na órbita da cooperação, como acontece com o CECCD da OTAN. Sem uma organização semelhante, ou mesmo sem a constituição de estruturas organizacionais que sejam compartilhadas por todos, não será possível sequer o cumprimento dessa condição.

Grau	Medidas
3º Grau	Dotação orçamental suficiente. Essa condição responde a uma realidade regional de desigualdade, de carências e de profundas e contínuas crises em diferentes países da região. Localmente, cada Estado pode criar estruturas consistentes e resilientes, mas no âmbito corporativo da América do Sul, a maioria dos países devem estar em condições de fornecer dotações orçamentárias suficientes aos sistemas para que, no conjunto, a região seja ciber-resiliente.

Fonte: O Autor

4.5 QUAIS FATORES PERMITEM E LIMITAM O PROCESSO DE POLÍTICAS NO CASO PARTICULAR DA AMÉRICA DO SUL?

No caso específico da América do Sul, os fatores que permitem ou limitam o processo de políticas é muito diverso e heterogêneo. Considerando o proposto por Dolowitz e Marsh (2000), e a conveniente revisão de Benson e Jordan (2011), a complexidade política regional abordada conjuntamente é a grande síntese do problema. Mesmo assim, a viabilidade pode se ver comprometida pelas ideologias existentes, pela disparidade tecnológica entre os países membros e pela burocracia própria das estruturas dos estados. Entretanto, a linguagem constitui uma grande vantagem sendo que o único país da região que fala uma língua diferente é o Brasil, sendo dita língua inteligível para a hispânica.

Atualmente, segundo o que foi apresentado, a falta de maturidade e cooperação regional são os principais óbices da articulação de um modelo comum. O problema existe, nenhum país pode fugir disso, mas ainda existem diversos problemas estaduais, regionais e muitas vezes ideológicos, que fazem com que essa cooperação necessária crie óbices no decorrer do caminho da eficiência.

Como foi apresentado por vários especialistas, a América do Sul vive a mesma situação que a Europa, enquanto que a ameaça cibernética não distingue fronteiras, nem soberania. Assim, deveria se tentar e puder assumir o

desafio. Ou seja, hoje, o principal obstáculo está sendo simplesmente a cooperação.

5. CONSIDERAÇÕES FINAIS

O estudo apresentado assume relevância porque procura identificar um mecanismo causal e as condições de necessidade e suficiência para construir um sistema cibernético resiliente no âmbito da América do Sul, avaliando as práticas do Centro de Excelência Cooperativo de Defesa Cibernético da OTAN, na Estônia.

Dita relevância mostrou-se incrementada a partir dos aportes oferecidos pelos quase 60 especialistas na matéria consultados, que fizeram parte da pesquisa, afastando-se então os resultados de uma visão meramente pessoal para se constituir em um consenso de um conglomerado significativo de conhecedores da área.

A concatenação e a estruturação da pesquisa, da maneira que foi feita, permitiu o melhor entendimento e a construção metodológica do resultado, iniciando com o referencial teórico que deu o marco devido; uma abordagem da Estônia como exemplo de vítima e ator fundamental dessa mudança de paradigmas na nossa Era da Informação e a evolução da OTAN em matéria de cibernética a partir da criação do CECCD; a construção do modelo de resiliência cibernética a partir dos dados obtidos da OTAN submetidos à análise e julgamento de quase 60 especialistas na área; e a apresentação de um caminho de transferência de políticas públicas da OTAN à OEA procurando que esse modelo seja aplicável na América do Sul.

A aplicação do *process tracing* como técnica metodológica, estabelecendo o mecanismo causal derivado do mapeamento histórico dos eventos que permitiram estabelecer variáveis as quais, submetidas à revisão dos especialistas, possibilitaram a formulação de condições, subcondições e componentes (aplicando a técnica literária de análise de condições causais), que, categorizando-as em necessárias, suficientes, INUS e SUIN, deram marco ao modelo criado de resiliência cibernética, somado à aplicação da literatura de transferência de políticas para testar as possibilidades (ou não) de encaixar ele

na América do Sul, resultou um grande ganho no processo racional necessário para chegar a conclusões relevantes.

O emprego da Estônia como ferramenta para entender a evolução da OTAN na área permitiu não só demonstrar com um exemplo concreto o que é a resiliência propriamente dita, más também desenvolver os conceitos de cooperação, integração, comprometimento nacional, regional e global, condições essas essenciais para progredir nessa órbita da cibernética.

A identificação dos componentes essenciais que poderiam transformar um sistema em ciber-resiliente, a partir da avaliação das medidas adotadas pela OTAN para com seus estados membros, representou o início do caminho de construção do modelo.

Para o desenvolvimento do modelo de resiliência cibernética, partindo do modelo criado a partir da análise das medidas que têm sido adotadas pela OTAN na Europa, foram consultados 58 especialistas na área (muitos dos quais são de altíssimo nível), representantes dos seguintes países: Argentina, Brasil, Chile, China, Colômbia, El Salvador, Equador, Espanha, Estados Unidos de América, Guatemala, México, Paraguai, Peru e Uruguai. Eles constituíram um verdadeiro ganho no nível e qualidade do estudo.

O dinamismo oferecido pelo quadro de síntese de resultados dos questionários de pesquisa dos especialistas, caracterizado por ter sido feita uma ponderação particularizada das opiniões deles e estabelecida uma categorização dos resultados obtidos, permitiu de fato construir a árvore de condições segundo o grau de relevância que cada uma delas representa no modelo.

Para incrementar o modelo foram analisadas e exploradas as respostas dos especialistas e, a partir da relevância e pertinência dos aportes feitos por eles foram identificadas mais duas sub-condições e diversos componentes a mais, convenientemente detalhados no modelo final de condições, sub-condições e componentes necessários para que um sistema possa ser considerado como ciber-resiliente (QUADRO 6).

Esse novo modelo criado à luz das experiências da OTAN e do questionário de pesquisa avaliado por especialistas, incrementado com o próprio aporte deles em respeito a componentes que não poderiam faltar, teve

que ser submetido a mais uma análise diferenciada para procurar sua transferência à América do Sul.

Considerando que a base do modelo provém de um organismo internacional que tem uma estrutura que possibilita sua implementação (OTAN), teve que ser identificada na América do Sul uma organização internacional que se constitua em análoga. Analisou-se então a UNASUL, o PROSUL e a OEA como possíveis receptores desse modelo, obtendo o voto de confiança a OEA como a OTAN.

Considerou-se também, a partir do enfraquecimento da UNASUL e a falta de estrutura do PROSUL, que é possível perceber o recente crescimento da OEA em matéria de cooperação e integração regional na área cibernética surgiu a partir da necessidade ou intenção de ocupar os espaços vazios que as organizações internacionais anteriormente mencionadas deixaram livres. Para materializar isto foram detalhadas uma série de notícias oficiais sobre a participação da OEA em países da região, sua relevância e compromisso nesse âmbito. Isto permitiu que seja confirmada a OTAN como análoga.

Nessas notícias apresentadas foi possível identificar uma série de condições do modelo que foram tratadas e desenvolvidas nos respectivos foros, entre as quais se encontram: gestão de risco e de mudança; processos contínuos e operacionais em qualquer circunstância; desenvolvimento de exercícios e modelos de simulação; cooperação privada, estadual, nacional e regional; formação e especialização de capital humano; e implantação e atualização das estratégias de resiliência cibernética (ciclo de vida).

Antes de submeter o modelo ao processo de transferência de políticas públicas entre a OTAN e a OEA, foram analisadas as diversas visões dos especialistas consultados ao respeito, obtendo como resultado uma porcentagem muito alta de profissionais que consideraram esse processo como fatível e uma mínima quantidade que acharam que não seria possível essa transferência.

Com todas as informações trabalhadas ao longo do estudo efetuou-se o processo de resposta dos interrogados que a literatura de *policy transfer* oferece como boa prática para fazer, sintetizados em:

- Por que se pretende que atores participem na transferência de políticas no âmbito da resiliência cibernética?
- Quem são os atores chave envolvidos no processo de transferência de políticas entre a OTAN e a América do Sul?
- O quê se pretende transferir e de onde foram extraídas as lições para seja feita?
- Quais são os diferentes graus de transferência e qual sua possível projeção no tempo?
- Quais fatores permitem e limitam o processo de transferência de políticas no caso particular da América do Sul?

Como resultado geral, após dar resposta aos interrogados, concluiu-se que é possível a transferência do modelo surgido na OTAN para o âmbito da OEA, mas com uma gradação diferenciada no tempo, a partir de três níveis de prazos.

Finalmente, e considerando a questão de estudo que norteou o trabalho (**a partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernético da OTAN, quais são as condições necessárias que conduzem à resiliência de sistemas cibernéticos e como estas práticas podem se transferir ao âmbito da América do Sul?**) e o objetivo principal proposto (**compreender, a partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernético da OTAN, quais são as condições necessárias que conduzem à resiliência de sistemas cibernéticos e como estas práticas podem se transferir ao âmbito da América do Sul**), pode se concluir que foram atingidos os objetivos propostos para o trabalho e que foi possível levantar resultados relevantes e aplicáveis a uma realidade regional não tão sólida e robusta, mas que se vislumbra próspera e otimista, deixando o caminho aberto para futuros estudos que levem à aplicação desse possível modelo teórico criado à prática.

REFERÊNCIAS

AGUIRRE, J. **Mecanismos causales y process tracing. Una introducción**. Mendoza: SAAP, Vol. 11, Nº 1, 2017.

ALZUGARAY TRETO, C. Nuevo regionalismo e integración regional en América Latina y el Caribe. Espanha: **Cursos de Derecho Internacional y Relaciones Internacionales, Servicio Editorial Universidad del País Vazco**, pp. 47-79, 2002.

ARGENTINA. **Presidência da Nação**. Organizamos capacitación internacional sobre ciberseguridad junto a la OEA. Mensagem publicada no portal da Presidência da Nação Argentina em 03 de agosto de 2018. Disponível em <https://www.argentina.gob.ar/noticias/organizamos-capacitacion-internacional-sobre-ciberseguridad-junto-la-oea>. Acesso em: 25 de julho de 2019.

ARGYRIS, C.; SCHON, D. **Theory in practice-increasing professional effectiveness**. San Francisco: Jossey – Bass Inc., 1994.

AVIAR, P. **A situação nas ruas é calma**. Tallin, Estônia: Eesti Päevaleht, 2007.

BEACH, D. **Process- Tracing Methods : Foundations and Guidelines**. First ed. Michigan, United States of American: The University Michigan Press, 2013.

BEACH, D. It ' s all about mechanisms – what process-tracing case studies should be tracing should be tracing. **New Political Economy**, [S.l.]: v. 3467, n. February, 2016.

BEAUDOIN, L.; JAPKOWICZ, N.; e MATWIN, S. **Autonomic Computer Network Defence Using Risk State and Reinforcement Learning**. New York: Cryptology and Information Security Series, v.3, pp.238-248, 2009.

BENNET, B. **Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infraestructure and Personnel**. New Jersey: Wiley - Interscience, 2007.

BENNET, C.; HOWLETT, M. **The Lessons of Learning: Reconciling Theories of Policy Learning and Policy Change.** Netherlands: Kluwer Academic Publishers, 1992.

BENSON, D.; JORDAN, A. What Have We Learned from Policy Transfer Research? Dolowitz and Marsh Revisited. London: **Political Studies Review**, Vol 9, p. 366-378, 2011.

BERINATO, S.; PERRY, M. As tendências da segurança em números. [S.l.]: **Hardvard Business Review Brasil**, 6 de julho de 2018. Disponível em https://hbrbr.uol.com.br/tendencias-seguranca-cibernetica/

BISQUERRA, R. **Métodos de investigación educativa. Guía práctica**. Barcelona: Grupo Editorial CEAC, 1989.

BORGOÑÓN, R. **La Antifragilidad – Esquema de su aplicación en el Arte y Método de Diseño Operacional.** Buenos Aires: Escuela Superior de Guerra Conjunta, 2017.

BRASIL. **Ministério de Relações Exteriores**. Disponível em: <http://www.itamaraty.gov.br/pt-BR/politica-externa/integracao-regional/14394-a-organizacao-dos-estados-americanos>. Acesso em: 08 de agosto de 2019.

BUCHAREST SUMMIT DECLARATION. Bucharest: Declaration issued by the Heads of State and Government participing the meeting of the North Atlantic Council, 2008.

BUSINESS CONTINUITY INSTITUTE. **Informe de exploração das perspectivas de futuro (*Horizon Scan*).** [S.l.]: BCI, 2018. Disponível em

http://medios.icontec.org/documentos/BCI-Horizon_Scan_Report-2018-letter.pdf

CANONGIA, C.; MANDARINO, R. **Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications**. Hershey: PA, IGI, 2014. Disponível em http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

CAPORASO, J,; PELOWSKI, A. Economic and political integration in Europe: a time series quasi-experimetal analysis. Estados Unidos: **American Political Science Review**, p. 421, 1975.

CARVAJAL CONTRERAS, M. **Derecho Aduanero**. México: Editorial Porrúa, p. 40, 1993.

CARVAJAL VILLAPLANA, A. Teorías y modelos: formas de representación de la realidad. Costa Rica: **Escuela de Ciencias Sociales del Instituto Tecnológico de Costa Rica**, p. 8, 2012.

CARAYANNIS, E. G.; CAMPBELL, D. F. J. **Cyber- Development , Cyber-Democracy and Cyber-Defense; Challenges, Opportunities and Implications for Theory, Policy and Practice**. New York: Springer, 2014.

CARRASCO, L. **Ciber-Resiliencia.** Madrid, Espanha: Instituto Espanhol de Estudos Estratégicos, 2015.

CASTELLANOS, W. Retos de Gestión de Riesgo Cibernético en la Transformación Digital.[S.I.]: **Dolitte LLP and Affiliated entities**, 2019. Disponível em https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Retos%20cyber%20risk%2026-feb-2019.pdf

CCDCOE NATO. **National Cyber Security Framework Manual**. Tallin, Estonia: 2012.

CESEDEN. **Concepto de defensa resumen ejecutivo**. Madrid, Espanha: Estado Mayor de la Defensa, 28 de septiembre de 2018. Disponível em http://www.emad.mde.es/Galerias/EMAD/files/Concepto_CIBER_Resumen_Ejecutivo.pdf

CHALMES, A. **What is the thing called science?** Queensland, Australia: Hackett Publishing Company, Inc., 1999.

CHILE. **Secretaria de Cibersegurança.** Comunicado de imprensa. Mensagem publicado em 06 de março de 2019. Disponível em <https://www.ciberseguridad.gob.cl/noticias/anuncian-fecha-para-simposio-de-ciberseguridad-de-la-oea-en-chile/>. Acesso em: 27 de julho de 2019.

CHILE. **Ministro de Relações Exteriores** (Teodoro Ribera). Mensagem enviada ao portal Noticias de América Latina y el Caribe em 18 de julho de 2019 por Teodoro Ribera, Ministro de Relações Exteriores do Chile. Santiago de Chile, 2019.

CLARKE, R.; KNAKE, R. **Guerra en la red, los nuevos campos de batalla**. Barcelona: Editorial Planeta, 2011.

CONTI, G.; SURDU, J. **Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?.**[S.l.]: Springer, Vol. 12, No. 1, p. 17, 2009.

CORLETTI ESTRADA, A. **Estratégia de segurança informática por camadas, aplicando o conceito de Operação Militar por Ação Retardante**. Madrid, Espanha: Tese (Doutorado em Informática) Universidade Nacional de Educação a Distância - Escola Técnica Superior de Engenharia Informática, 2011.

CORLETTI ESTRADA, A. **Ciberseguridad: Una Estrategia Informático-Militar**. Primeira ed. Madrid: DarFe, 2017.

CZOSSECK, C.; GEERS, K. **The Virtual Battlefeld: Perspectives on Cyber Warfare**. Tallinn: IOS Press BV, 2009.

CZOSSECK, C.; OTTIS, R.; TALIHARM, A. **Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security**. Sydeny: International Journal of Cyber Warfare and Terrorism, 2011.

DOLOWITZ, D. P.; MARSH, Y. D. Learning for abroad : The rule of policy transfer in the actual politics decitions. **Dolowitz y Marsh Revisited**. [S.l.]:v. 13, n. 1, 2000.

DONALDSON, S.; SIEGEL, S.; WILLIAMS, C.; ASLAM, A. **Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats**. New York: [s.n.].

ECONOMY, T. P.; POWERS, S. M.; JABLONSKI, M. **The Real Cyber War**. Urbana, Chicago and Sprinfield: University of Illinois Press, 2015.

FERRERO, J. **La ciberguerra. Génesis y evolución**. Madrid: Revista General de la Marina, 2013.

FM GLOBAL. **Research and Resources**. [S.l.]: FM Global, 2019. Disponível em: https://www.fmglobal.com/research-and-resources.

GAMERO, A. **Cyber Conflicts in International Relations: Framework and Case Studies.** Estados Unidos: Seminario sobre “Cyber International Relations”, 2014.

GARCÍA-AJOFRIN, L. **Gigantes de la Educación: lo que no dicen los rankings**. Madrid: Editorial Ariel – Fundación Telefónica, 2016.

GEERS, K. **Strategic Cyber Security. NATO Cooperative Cyber Defense Centre of Excelence**. Estônia: Seminário, 2011.

GÓMEZ, M. Link para consultas dos 58 questionários de pesquisa formulados. Disponível em: <https://drive.google.com/drive/folders/132aQxeKMsrgIFNRWZbddLkDJ8f2eUKK3?usp=sharing>. Acesso em: 07 de agosto de 2019.

GROTBERG, E. **Introdução: novas tendências em resiliência**. Wisconsin: Universidad de Wisconsin, 1995.

HARRINGTON, A.; THEOHARY, C. **Cyber Operations in DOD Policy and Plans: Issues for Congress. Congressional Research Service. CRS Report – Prepared for Members of Commitees of Congress.** Estados Unidos: Congresso dos Estados Unidos, 2015.

HOUGH, P; MALIK, S.; MORAN, A.; PILBEAM, B. **International Security Studies: Theory and Practice**. London, 2015.

HUTCHINS, E. **Cognition in the Wild**. Cambridge: MIT Press, 1995.

INFANTE, F. A **resiliência como processo: uma revisão da literatura recente**. Tradução Valério Campos. Porto Alegre: Artmed, 2005.

INTECO. **Resiliencia: Aproximación a um marco de medición**. Madrid: CERT de Segurança e Indústria – INTECO: Instituto nacional de Tecnologías de las Comunicaciones, 2018.

ISACA. **Cyber News**. [S.l.]: ISACA, 2019. Disponível em: https://www.isaca.org/Pages/default.aspx?cid=1210069&Appeal=SEM&gclid=CjwKCAjwvbLkBRBbEiwAChbckZ6Nibf1rC-MfTlewIuVSL3met0i2iLqS042UA-I4oy9BzV889_xlhoCypoQAvD_BwE&gclsrc=aw.ds

ITU. **Global Cyber Security Index 2017 (GCI).** [S.l.]: International Telecommunications Union, 2017. Disponível em https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf

ITU. **Guide to developing a National Cyber security Strategy.** Outubro de 2018. Disponível em: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

ITU. **Overview of Cybersecurity. Recommendation ITU-T X.1205**. Geneva: International Telecommunication Union (ITU), 2009. Disponível em http://www.itu.int/rec/T-REC-X.1205-200804-I/en

ITU. **Resolución 181.** Noviembre de 2010. Disponível em: https://www.itu.int/net/itunews/issues/2010/09/20- es.aspx

JID. Comunicado de prensa. Mensagem publicado em 28 de novembro de 2018. Disponível em <http://www.jid.org/?p=2662>. Acesso em: 27 de julho de 2019.

JORDAN, T. **Cyberpower: the culture and politics of cyberspace and the internet**. Washington DC: Library of Congress, 2003.

JORDANA, J.; LEVI-FAUR, D.; FERNÁNDEZ, J. **The Global Diffusion of Regulatory Agencies: Channels of Transfer and Stages of Diffusion**. New York: Comparative Political Studies, vol. 44, 201.1

KEMMERER, R. **Cybersecurity**. [S.l.]: 25th IEEE International Conference on Software Engineering: p 705-715, 2003.

KLIMBURG, A. **National Cyber Security: Framework Manual**. Estonia: NATO Cooperation Cyber Defense Centre of Excelence, 2014.

LADRIÈRE, J. **El reto de la racionalidad. La ciencia y la tecnología frente a las culturas**. Salamanca: UNESCO /Sígueme, 1978.

LEVI-FAUR, D**. The Global Diffusion of Regulatory Capitalism**. New York: The annals of the American Academy of Politician and Cocial Science, Vol 598, 2005.

LEWIS, J. **Cybersecurity and Critical Infrastructure Protection**. Washington, DC: Center for Strategic and International Studies, 2006.

LLONGUERAS, A. **La guerra inexistente, la ciberguerra**. Madrid: Editorial Acad MIA Espa Ola, 2013.

MAHONEY, J; RUESCHEMEYER, D. **Comparative Historical Analysis in the Social Sciences**. New York: Cambridge University Press, 2003.

MAHONEY, J.; GOERTZ, G. **A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research**.[S.l.]:n. 0093754, p. 227–249, 2006.

MAHONEY, J. Process Tracing and Historical Explanation. **Security Studies**, [S.l.] 2015.

MALHOTRA, N. [et al]. **Introdução à pesquisa de marketing**. São Paulo: Pearson Prentice Hall, 2005.

MELILLO, A.; SUAREZ OJEDA, E. **Resiliência: descobrindo as próprias fortalezas (2001)**. Tradução de Valério Campos. Porto Alegre: Artimed, 2005.

MEJIAS, S. La OEA: un actor regional en la gestión de crisis. Logros y limitaciones. Madrid: **Adenda**, pp 69-98, 2008.

MC NAMARA, S. **NATO summit 2010: Time to Turn Words Into Action**. Washington DC: The Hertiage Foundation. Backgrounder, 2010.

MINTZBERG, H. **Mintzberg on Management: Inside our Strange Word of Organizations**. New York, The Free Press, 1989.

NEWMEYER, K. **Ciberespaço, Cibersegurança e Cyberwar**. Lima, Perú: II Simpósio Internacional de Segurança e Defesa, 2015.

NETO, O.; COSSIO RIDRIGUEZ, J. O novo método histórico-comparativo e seus aportes à ciência política e à administração pública. **Revista de Administração Pública**, [S.l.]:v. 50, n. 6, p. 1003–1027, 2016.

NYE, J.; WELCH, D. Un**derstanding Global Conflict and Cooperation, an Introduction to Theory and History**. Boston, Pearson, 9th Edition, 2013.

OBINGERA, H.; SHMITTA, C.; STARKEA, P. Policy Diffusion and Policy Transfer in Comparative Welfare State Research. Bremen, Germany: **Social Policy & Administration**, Vol. 47, No. 1, 2013.

O´CONNOR, K. **The History of the Baltic States**. Wesport: Greenwood Press, 2003.

OEA. Disponível em: <http://www.oas.org>. Acesso em: 05 de agosto de 2019.

OEA. Comunicado de imprensa. Mensagem publicado em 23 de setembro de 2018. Disponível em <http://www.oas.org/es/centro_noticias/comunicado _prensa.asp?sCodigo=AVI-130/18>. Acesso em: 23 de julho de 2019.

OEA. Comunicado de imprensa. Mensagem publicado em 24 de outubro de 2018. Disponível em <http://www.oas.org/es/centro_noticias/comunicado _prensa.asp?sCodigo=C-065/18>. Acesso em: 25 de julho de 2019.

OEA; CIDH. **Libertad de expresión e Internet.** 31 de dezembro de 2013. Disponible en (PDF): https://www.oas.org/es/cidh/expresion/docs/informes/ 2014_04_08_internet_web.pdf

OTAN. Strategic Foresight Analysis 2015. Bruxelas, 2015. Disponível em: <https://www.act.nato.int/images/stories/media/doclibrary/160121sfa.pdf>. Acesso em 08 de agosto de 2019.

OTAN. Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council. Bruxelas, 2016. Disponívem em: <https://www.nato.int/cps/en/natohq/official_texts_133180.htm>. Acesso em 08 de agosto de 2019.

OTAN. Defense College. The evolution of the Hibrid Threat and Resilience as a Conuntermeasure. Bruxelas: Nro 139, 2017.

OTAN-UE. Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Bruxelas, em 8 de julho de 2016. Disponívem em:<https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160708_160708-joint-NATO-EU-declaration.pDf>. Acesso em 08 de agosto de 2019.

OTAN-UE. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Bruxelas, em 6 de dezembro de 2016. Disponívem em:< http://www.nato.int/cps/en/natohq/official_texts_138829.htm>. Acesso em 08 de agosto de 2019.

OTTIS, R. **Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective.** Tallin: Corporative Cyber Defence Center of Excellence (CCDCOE), 2008.

OTTIS, R.; LORENTS, P. **Cyberspace: Definition and Implications**. Tallin, Estonia: Cooperative Cyber Defence Centre of Excellence, 2012.

PARAGUAI. **Ministro de Relações Exteriores** (Rodolfo Nin Novoa). Mensagem publicada no portal do Ministério de Relações Exteriores do Paraguai em 14 de dezembro de 2018 por Rodolfo Nin Novoa, Ministro de Relações Exteriores do Paraguai. Assunção, 2018.

PELTON, J.; SINGH, I. **Digital Defense: A Cybersecurity Primer**. New York: Springer, 2015.

PIEDRA, D. Lecciones de aprendizaje, transferencia de políticas y la difusión internacional de la política Ideas. **Centrer for the Study of Globalisation and Regionalisation**, [S.l.]:p. 41, 2001.

POLETTI, R.; DOBBS, B. **A resiliência: a arte de dar a volta por cima**. Tradução de Stephania Matousek. Petrópolis, RJ: Vozes, 2007.

PUCHALA, D. Of blead men, elephants and international integration. Londres: **Journal of Common Market Studies**, X-No 3, p. 277, 1972.

RELIA, S. **Cyber Warfare: Its Implications on National Security**. New Delhi: Vij Books India Pvt Ltd, 2015.

RICHARDS, J. **Cyber-War: The Anatomy of the Global Security Threat**. London: Palgrave Pivot, 2014.

RODRIGUES, K. F.; RODRIGUES, I. S. Process tracing: o método, inovações e perspectivas para o campo da Administração Pública. **V Encontro Brasileiro de Administração Pública - Universidade Federal de Viçosa**, [S.l.]: p. 15, 2017.

ROWLAND, J.; RICE, M.; SHENOI, S. The anatomy of a cyber power. [S.l.]: **International Journal of Critical Infrastructure Protection**, Sv. 7, n. 1, p. 3–11, 2014.

RUDIO, F. **Introdução à pesquisa científica**. São Paulo: Livraria Grandes Editores ltda, 1978.

SABATIER, P.; JENKINS-SMITH, H. **The Advocacy Coalition Framework: Assessment, Revisions and Implications for Scholars and Practitioners.** Boulder: Westview Press, 1993.

SABATINI, C.; ALBERTONI, N. Prosur y el mito de la integración latinoamericana. **New York Times**, New York, 29 de março de 2019. Disponível em: <https://www.nytimes.com/es/2019/03/29/prosur-america-latina/>. Acesso em: 25 de julho de 2019.

SAMPIERI, R.; FERNÁNDEZ COLLADO, C.; BAPTISTA LUCIO, P. **Metodología de la Investigación**. 6ta Ed ed. México DF: Mc Graw Hill Education, 2014.

SANCHEZ, F [et al]. **Psicología Social**. Madrid: McGraw-Hill, 1993.

SCHMITT, M. **Tallinn Manual on the International Law Applicable to Cyber Warfare**. New York, United States of America: Cambridge University Press, 2013.

SENGE, P. **La quinta disciplina en la práctica: estrategias y herramientas para construir la organización abierta al aprendizaje.** Buenos Aires, Ediciones Granica S.A, 2006.

SERRANO, A.; MARTINEZ, E. **La Brecha Digital: Mitos y Realidades**. México: UABC, 2003.

SHANNON, R. **Simulación de Sistemas. Diseño, desarrollo e implementación**. México: Trillas, 1988.

SIERRA, D. Las dos caras de la tecnología. [S.l.]: **Informe mensual de ciberseguridad**, v. 2, p. 16, 2015.

SIERRA BRAVO, B. **Ciencias sociales. Epistemología, lógica y metodología**. Madrid: Paraninfo, 1988.

STEL, E. **Guerra Cibernética**. Buenos Aires: Círculo Militar, 2005.

SUAREZ, E.; MELILLO, A. **Resiliencia: Descubriendo las propias fortalezas**. Buenos Aires: Paidós, 2005.

SUNKEL, A. ; PAZ, J. **El subdesarrollo latinoamericano y la teoría del desarrollo.** México: Editorial Siglo 21, pp. 15-268, 1981.

TADDEO, M.; GLORIOSO, L. **Ethics and Policies for Cyber Operations. A NATO Cooperative Cyber Defence Centre of Excellence Initiative**. Switzerland: Springer International Publishing, 2017.

TALEB, N. **The Black Swam. The Impact of the Highly Improbable**. New York: Paidos Ibérica, 2007.

TALEB, N. **Antifragile: things that gain from disorder**. New York: Random House, 2012.

Tallinn Manual on the International Law Appicable to Cyber Warfare.New York: Cambridge University Press, 2013.

TAVARES, J. **Resiliência e educação**. 2.ed. São Paulo: Cortez, 2001.

TIKK, E.; KASKA, K.; VIHUL, L. **International Cyber Incidents. Legal Considerations.** Tallinn: Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.

TRATADO DEL ATLÁNTICO NORTE. Washington DC: Tratado assinado entre os Estados firmantes, 1949.

UE. **Parlamento Europeio.** Comunicação da Comissão ao Parlamento Europeio e ao Conselho sobre “O planejamento da UE sobre a resiliência e a

redução do risco de catástrofes nos países em desenvolvimento: aprender das crises alimentarias", em 3 de outubro de 2012. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=//EP//TEXT+REPORT+A7-2013-0375+0+ DOC+XML+V0//ES>. Acesso em 08 de agosto de 2019.

UE. **Parlamento Europeio**. Action Plan for Resiliencie in Crisis Prone Countries 2013-2020. Bruxelas, 2013. Disponível em: <https://ec.europa.eu/echo/files/policies/resilience/com_2013_227_ap_crisis_prone_countries_en.pdf>. Acesso em 08 de agosto de 2019.

UNASUR. **Tratado Constitutivo de la Unión de Naciones Suramericanas**. Entrada em vigor em 11 de março de 2011. Disponível em: https://www.unasursg.org/images/descargas/DOCUMENTOS%20CONSTITUTIVOS%20DE%20UNASUR/Tratado-UNASUR-solo.pdf. Acesso em: 08 de agosto de 2019.

VAN CREVELD, M. **Technology and War: From 2000 B.C. to the Present.**Washington: Simon and Schuster, p. 246, 2010.

VERGARA, S. **Métodos de pesquisa em administração**. São Paulo: Atlas, 2008.

WARTOFSKY, M. **Introducción a la filosofía de la ciencia**. Madrid: Alianza editorial, 1983.

WEYLAND, K. **Bounded rationality and policy diffusion: social sector reform in Latin America**. New Jersey: Princeton University Press, 2006.

WILLIAMS, B. The Joint Force Commander´s Guide to cyberspace Operations. Unites States: **Joint Force,** Quarterly 73, p. 14, 2014.

ZIOLKOWSKI, K. (ed.). **Peacetime Regime for State Activities in Cyberspace**. Tallinn: International Relations and Diplomacy, NATO CCD COE Publication, 2013.

APÉNDICE A – Esquema Gráfico de Pesquisa

ESQUEMA DE PESQUISA - MAJOR MARIANO OSCAR GÓMEZ					
Título	**Procurando um modelo de resiliência cibernética baseado nas experiências da OTAN e sua possível transferência na América do Sul**				
Problema	**A partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN, quais são as condições causais que conduzem à resiliência de sistemas cibernéticos e como estas práticas podem se transferir ao âmbito da UNASUL?**				
Obj. Princ.	**Compreender, a partir das práticas do Centro de Excelência Cooperativo de Defesa Cibernética da OTAN, quais são as condições causais que conduzem à resiliência de sistemas cibernéticos e sua possível transferência ao âmbito da UNASUL**				
Introdução					
Ítems a desenvolver	Questão de Estudo	Objetivos	Delimitação do Estudo	Relevância	Estrutura de Pesquisa
Cap 1	**Referencial Teórico e Metodológico**				
Conceito	Esse capítulo deve conter o marco teórico que fundamenta os temas a desenvolver.				
Ítems a desenvolver	Introdução ao Marco Referencial Teórico	Cibernética, conceitos de definições	Cooperação e Integração Internacional	Modelos	Transferência de Políticas
	Tipo de Pesquisa	Coleta de Dados	Plano de Pesquisa		
Cap 2 - Obj. Esp. 1	**A OTAN e a Ciber-Resiliência. Objetivo: Compreender o princípio da resiliência e seus componentes essenciais como alvo a ser atingido pela OTAN na sua estrutura cibernética**				
Conceito	Serão desenvolvidas com maior detalhamento as diferentes definições de Resiliência, sua importância no âmbito cibernético e a evolução que tem tido a Estônia neste sentido a partir da criação do CECCD da OTAN				
Ítems a desenvolver	Princípio de Resiliência	Evolução da Estônia no campo cibernético até o ciber ataque massivo de 2007	Medidas adotadas pela Estônia e pela OTAN depóis do ciber ataque massivo de 2007	Componentes essenciais que poderiam transformar um sistema em ciber-resiliente	Considerações parciais
Cap 3 - Obj. Esp. 2	**Procurando um modelo Ciber-Resiliente. Objetivo: Delinear quais são as condições causais, elementos constituintes de sistemas resilientes e suas respectivas relações de necessidade e suficiência**				
Conceito	Para determinar quais destas condições são necessárias e suficientes (ou combinações dos mesmos derivada), vai ser submetida a uma avaliação dos expertos e especialistas que conceituarão o grau de importância de cada um (1 a 7) a partir da formulação de questionários. Esta será a parte quantitativa da pesquisa. A partir da análise dos dados coletados, os mecanismos causais serão estabelecidos com base nos limites da pesquisa estabelecida, utilizando o ProcessTracing dentro do modelo de pesquisa qualitativa. Para isso:				
Ítems a desenvolver	Especialistas a serem consultados	Estatísticas obtidas dos resultados dos questionários realizados	Análise dos resultados obtidos	Criação de um modelo de resiliência cibernética	Considerações parciais

Cap 4 - Obj. Esp. 3	**É Possível uma América do Sul Ciber-Resiliênte? Objetivo: Analisar em que medida estes parâmetros internacionais foram ou podem ser importados pela América do Sul de maneira efetiva, conforme à literatura de Policy Transfer**				
Conceito	Como subseqüente etapa da pesquisa, as medidas adotadas no campo da ciberdefesa pela América do Sul serão analisadas, e sua devida conjuntura, para confirmar se existe alguma possibilidade de importar para a região o modelo de ciber-resiliência aplicado pela Estônia e na execução da OTAN. Será empregada literatura referida a Policy Transfer, também no âmbito da pesquisa qualitativa. Para fazer isso:				
Ítems a desenvolver	Análise da situação particular da América do Sul em quanto às medidas adotadas no âmbito cibernético	Situação de cooperação regional em matéria cibernética	Emprego da literatura de transferência de políticas públicasno caso de estudo	Considerações sobre a possibilidade (ou não) de aplicação do modelo criado no âmbito da América do Sul	
Concl.	**Conclusões gerais sobre a pesquisa (Conclusões)**				
Ítems a desenvolver	A relevância que tem o princípio de Resiliência no campo cibernético baseado na experiência sofrida pela Estônia na sua evolução digital.	A importância do CECCD OTAN para se chegar a um modelo a resiliência cibernético de nível regional. A Cooperação Européia para o estabelecimento de padrões de excelência necessários para atingir a resiliência cibernética.	Os resultados de pesquisa realizada com especialistas sobre um modelo de ciber resiliência aplicável no marco do conglomerado de variáveis e condições, e sua devida catalogação para formar um mecanismo causal para chegar à formação de um modelo aplicável de ciber-resiliência.	O peso que é dado às resoluções regionais da OTAN para a aplicação de medidas no campo cibernético.	A possibilidade (ou não) de aplicação de um modelo cibernético exportável de uma situação, um contexto diferente e mais evoluído.

APÉNDICE B – PROCESSO DE ELABORAÇÃO DO QUESTIONÁRIO

Para a elaboração do questionário foi empregada a técnica desenvolvida por Malhotra (2005), aplicável ao caso de estudo, considerando os seguintes passos:

1. Especificar as informações necessárias: baseado nos objetivos da pesquisa, o problema e a questão de estudo, o público-alvo deverá ser do nível adequado (da área de cibernética), com um adequado nível educacional e de experiência na disciplina, o que levará a que a linguagem empregada seja familiar para os entrevistados.

2. Especificar o tipo de método de entrevista: Questionário enviado por correio eletrônico de tipo auto-aplicativo, não envolvendo interação pessoal entre o entrevistador e o entrevistado.

3. Determinar o conteúdo de cada pergunta: Perguntas a serem feitas para a elaboração do questionários; a primeira é se essa pergunta que está sendo elaborada é necessária (em virtude dos dados resultantes); e a segunda é se são necessárias várias perguntas em vez de uma para o assunto a tratar.

4. Elaborar as perguntas para superar a falta de capacidade e de disposição do entrevistado em responder: Mesmo sendo os entrevistados profissionais que serão escolhidos minuciosamente por causa da suas capacidades e conhecimentos, é possível que o entrevistado responda alguma pergunta sem estar devidamente informado. Para isso será feita uma introdução de dados essenciais fornecidos por literatura de relevância para cada pergunta aos efeitos de orientar o leitor no problema em questão.

5. Elaborar as perguntas para superar a relutância do entrevistado em responder: Mesmo que o entrevistado consiga responder a uma pergunta específica, ele pode não querer fazê-lo por várias circunstâncias, pelo esforço que implica, pelo tipo de conteúdo a ser tratado, por ser perguntas de caráter pessoal, etc.). Na área de pesquisa que está sendo desenvolvida, o último dos pontos considerados como condicionantes será uma barreira que o pesquisador deverá ter muito em conta (informações exigidas muito delicadas).

Essa situação deverá ser analisada com detalhe para a elaboração do questionário.

6. Decidir sobre a estrutura das perguntas: No questionário serão empregadas principalmente perguntas estruturadas de múltipla escolha, finalizando com uma pergunta não estruturada na qual se deixará ao entrevistado a opção de adicionar mais algum condicionante ao modelo apresentado.

7. Determinar o texto das perguntas: Serão utilizadas palavras simples, claras e da linguagem comum da área, evitar palavras ambíguas e evitar criar perguntas que induzam respostas ou que sejam tendenciosas.

8. Colocar as perguntas na ordem apropriada: O questionário começará com perguntas pessoais referentes à função profissional do entrevistado. Continuará com uma pergunta de abertura, que preparará o cenário para o restante do questionário e tentará seguir uma abordagem de tipo funil invertido para a ordem das perguntas, iniciando com aquelas que sejam estreitas e específicas para chegar a perguntas gerais e conceituais.

9. Identificar o aspecto visual – formato e layout: As características físicas de um questionário, como formato, espaçamento e posicionamento, podem ter efeito significativo nos resultados. Por isso se tentará dividir o questionário em seções, com áreas de tópicos separados para cada uma, e com uma apresentação visual que ajude ao entrevistado na sua intenção de responder a pesquisa.

10. Reproduzir o questionário: Se procurará boa qualidade visual, evitando que as perguntas passem de uma página para a outra e a superposição de perguntas.

11. Eliminar as falhas com o pré-teste: Com esta etapa se procurará testar o questionário em uma amostra pequena de entrevistados para identificar e eliminar possíveis problemas.

APÉNDICE C – QUESTIONÁRIOS

O seguinte questionário responde a uma necessidade de validar as condições essenciais que um sistema deve reunir para se transformar em resiliência cibernética.

O questionário terá três partes, sendo a primeira orientada a estabelecer uma ficha pessoal do entrevistado, continuando com uma segunda parte com perguntas de caráter estruturadas relacionadas com a ponderação que o entrevistado dá a cada condição apresentada como necessária para que um sistema reúna as características de ser ciber-resiliente, e a terceira parte de caráter não estruturada, relacionada com a visão do entrevistado (especialista) respeito ao problema exposto, pudendo acrescentar, segundo sua experiência (conhecimento), mais condições que considere conveniente adiar.

Parte I: Dados Pessoais

Posto	
Nome e sobrenome	
Organização	
País	
Função atual	
Experiência na área (breve descrição)	

Parte II: Condições

A continuação será apresentada uma série de condições as quais se requer avaliação segundo o que o senhor considere mais relevante ou menos relevante (até inaplicável), para ser tido em conta na construção de um modelo de resiliência cibernética. Para isso, será empregada uma escala numérica de 1 até o 7, sendo o número 1 o menos relevante e o número 7 o mais relevante, pudendo escolher só um valor para cada condição.

. 1. **Condição:** ***Gestão de risco e de mudanças***. Beaudoin, Japkowicz e Matwin (2009) afirmam que a gestão de risco atinge o equilíbrio certo entre o custo das medidas adotadas e o benefício hipotético para a sua implantação. Ou seja, este tipo de gestão é quando se trata de ameaças. O gerenciamento de mudanças se refere à identificação de mudanças a serem feitas e os impactos organizacionais que devem ser tidos em conta para o processamento adequado. Ou seja, este tipo de gestão é quando se trata da evolução da exposição a eventos externos.

Escolha a ponderação que ache mais adequada:

	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

2. **Condição**: ***Conhecimento profundo da organização (interna e externamente)***. Para Senge (2006), alcançar o conhecimento real e profundo da organização é uma condição fundamental. Resiliência cibernética requer adaptabilidade e sobrevivência, por isso, é necessário conhecer a organização e o ambiente. Visão crítica interna e externa da organização.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

3. **Condição:Área da Cibernética com c*apacidade e participação no nível da organização de gerenciamento de tomada de decisão***. A teoria de Mintzberg (1989) estabelece que, para que um sistema consiga atingir o seu estado de resiliência, é necessária uma liderança harmoniosa e sinérgica de todos os níveis e componentes da organização em causa.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

4. **Condição:** ***Capacidade de antecipar a crise (CERT).*** Segundo Newmeyer (2015) essas capacidades são a chave para a resiliência.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

5. **Condição:*Simplificação de sistemas de informação para reduzir processos e interfaces***. Analisando a teoria de Pelton e Singh (2015), a estrutura, a base de arquiteturas sistemas materiais e relações humanas, devem ser tão simples quanto possível.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

6. **Condição:*Processos contínuos e operacionais em qualquer circunstância***. Segundo Estrada (2017), todo sistema informático é composto de infra-estrutura, hardware, software e processos, cada um com um nível de interferência particularizado, afetando em maior ou menor medida, o bom funcionamento da plataforma. Mas todos eles trabalham sinergicamente para

que, como um todo, possam se transformar em um sistema resiliente. Mas esse processo deve ser contínuo e operado sob quaisquer circunstâncias, distinguindo os processos que são essenciais e devem realizar escala de prioridades para o momento de ser temporariamente suspensos.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

7. **Condição:*Garantir regulamentos nas infra-estruturas críticas***. Os autores Rowland, Rice e Shenoi (2014), definem às infra-estruturas críticas como aquelas instalações, redes, serviços e equipamentos físicos e de tecnologia da informação cuja perturbação ou destruição teria um impacto maior sobre o funcionamento eficaz das instituições estatais e autoridades públicas. É por isso que é necessário que essas infra-estruturas críticas sejam adequadamente reguladas e padronizadas para garantir a proteção necessária.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

8. **Condição:*Estrutura de sistema de informação (hardware e software).*** Segundo Economy, Powers e Jablonski (2015) é necessário assegurar o desenho da segurança cibernética dos elementos que suportam os processos da organização. Exigência de compra (hardware e software) de sistemas padronizados. Funcionalidade e fiabilidade dos sistemas de tecnologia da informação e comunicações. Aumentar o nível de demanda para compra de equipamentos sem dividir a parte funcional da segurança do produto.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

9. **Condição:*Desenvolvimento de exercícios e modelos de simulação***. Analisando aos autores Carayannis e Campbell (2015) a simulação é necessária para verificar o nível de resiliência cibernético do sistema, a eficácia das medidas tomadas, e a avaliação da velocidade de resposta, a realização de exercícios e modelos de simulação, tanto seja no interior como no exterior do sistema, é necessária.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

10. **Condição:*A atualização do quadro legal.*** Segundo o "*Tallinn Manual on the International Law Appicable to Cyber Warfare*" (2011) é necessário harmonizar a legislação do ambiente cooperativo de políticas de segurança de rede e informações, bem como o estabelecimento de autoridades nacionais para a coordenação e ativação de CERT.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

11. **Condição:*Cooperação privada, estadual, nacional e regional***. Richards (2014) desenvolve o conceito que a cooperação entre as autoridades e agências de corpos de segurança e defesa é fundamental. Promover a cooperação e o intercâmbio de informações entre a indústria e os serviços de segurança cibernética.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

12. **Condição:*Ferramentas de desenvolvimento e melhoria contínua da segurança cibernética.*** Segundo Relia (2015) tem que ter principalmente em conta as ferramentas de desenvolvimento e melhoria militares, de inteligência e de aqueles que suportam sistemas de comunicação estrategicamente importantes. Este último, em cooperação com os operadores privados. Para este tipo de ferramentas é desejável que a produção nacional tanto seja para gerar o *know-how* de conhecimento, bem como para aperfeiçoar a blindagem no quadro local.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

13. **Condição:*A proteção física do patrimônio tecnológico***. Donaldson et al. (2014) consideram que os sistemas de infra-estruturas empregados em segurança cibernética representam um ponto extremamente vulnerável como portas de entrada para o sistema ou como peças necessárias para o

funcionamento harmonioso. A proteção física de tal patrimônio tecnológico também é essencial para alcançar a resistência desejada.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

14. **Condição:*Formação e especialização de capital humano***. Segundo Hough et al. (2015), e necessária a formação contínua e permanente de capital humano para adquirir a experiência necessária para a tarefa. Ambiente profissional qualificado e com níveis extremos de conhecimento sobre as diferentes capas de segurança.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

15. **Condição:*Implantação e atualização das estratégias de resiliência cibernética (ciclo de vida).*** Estrada (2017) considera que essas estratégias devem ser aplicadas à segurança de rede, nós e áreas, formando uma defesa cibernética em profundidade e altura. Planos de gestão de segmentação e serviços de rede. Estratégias tais como seguir e prosseguir ou proteger e proceder. Ou seja, todo o procedimento e as ações apropriadas para a implantação que salvaguarde e permitirá que a organização possa retornar a um estado operacional no menor tempo possível. Então será necessário adaptar todo o conjunto de medidas que estão disponíveis para a organização em intervalos apropriados (ciclo de vida).

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

16. **Condição:*Dotação orçamental suficiente***. Em referência com essa condição, a maioria da bibliografia consultada reforça a necessidade de contar com o orçamento adequado para a renovação e atualização de recursos humanos e materiais contínua para garantir a resiliência dos sistemas cibernéticos.

Escolha a ponderação que ache mais adequada:

1	Não aplica
2	Irrelevante
3	Pouco relevante
4	Medianamente Relevante
5	Relevante
6	Muito Relevante
7	Imprescindível

Parte III: Outras Considerações

1. Que outra/s condição/ões acha conveniente adiar à nomina descrita na Parte II do questionário, para a criação de um modelo ciber-resiliente. Dê um breve fundamento da sua/s escolha/s.

2. O senhor considera que essas condições necessárias para que um sistema possa alcançar a resiliência desejada, enunciadas na Parte II e Parte III (ponto 1.) da presente pesquisa, seriam aplicáveis ao marco cooperativo e corporativo da América do Sul? Dê uma breve justificativa a sua resposta.

APÊNDICE D – LISTA DE ESPECIALISTAS

ARGENTINA:

1. General de Brigada (EA - R) Gustavo Enrique Vázquez: Engenheiro Militar do Exército Argentino com mestrados feitos no Equador e na Argentina. Suas funções mais relevantes na área relacionada com o caso de estudo foram ter sido Comandante de Pelotão de Comunicações na Guerra das Malvinas, Comandante do Batalhão de Comunicações 602 (com responsabilidade na infra-estrutura crítica de TIC do Exército Argentino), Chefe do Departamento de Desenvolvimento da Diretoria Geral de Comunicações e Informática, Sub- Comandante da Diretoria Geral de Comunicações e Informática, Diretor Geral de Comunicações e Informática e finalmente Diretor Geral de Planos, Programas e Orçamentos do Exército, função na qual passou à Reserva em 2017.
2. Coronel (EA) Ernesto Balloffet: Oficial de Estado Maior do Exército Argentino e Licenciado em Informática. Suas funções principais na área foram ter sido Comandante do Batalhão de Comunicações 602 (com responsabilidade na infra-estrutura crítica de TIC do Exército Argentino), Chefe do Departamento Informática da Diretoria Geral de Comunicações e Informática e atualmente nomeado Diretor de Defesa cibernética do Exército Argentino.
3. Coronel (EA) Cicerchia: Oficial Engenheiro Militar com a especialização em Informática e Cibernética. Suas funções principais na área foram ter trabalhado desde sua fundação no Centro de Desenvolvimento de Software do Exército e ter trabalhado desde o inicio da sua criação no Comando Conjunto de Defesa cibernética como Chefe do Departamento Sistemas e como Chefe do Departamento Operações.
4. Coronel (EA) Luis Pablo Guimpel: Oficial de Estado Maior do Exército Argentino e do Exército Brasileiro, sendo também Licenciado em Informática. Suas principais funções na área foram ter sido Comandante do Esquadrão de Comunicações Blindado 2, Comandante do Batalhão de Comunicações 601 (com o qual foi deslocado em missão das Nações Unidas por um não na UNFICYP), e atualmente se desempenha como

Chefe do Departamento Operações do Comando Conjunto de Defesa cibernética.

5. Tenente Coronel (EA) Andrés Revetria: Oficial Engenheiro Militar, com mestrado no Instituto Tecnológico de Buenos Aires. Foi Chefe de Companhia de Redes e Sistemas e Subcomandante do Batalhão de Comunicações 602 (com responsabilidade na infra-estrutura crítica de TIC do Exército Argentino), trabalhou muitos anos da Diretoria Geral de Comunicações e Informática na área de TIC e atualmente se desempenha como professor da Escola Superior Técnica do Exército Argentino, no marco da Faculdade de Engenharia.
6. Major (EA) Raúl Machinandiarena: Oficial Engenheiro Militar com mestrado na Universidade Tecnológica Nacional. Suas principais funções na área foram ter sido Chefe de Companhia de Redes e Sistemas e Subcomandante do Batalhão de Comunicações 602 (com responsabilidade na infra-estrutura crítica de TIC do Exército Argentino), trabalhou muitos anos da Diretoria Geral de Comunicações e Informática na área de TIC e atualmente se desempenha como Chefe da Companhia de Comunicações Mecanizada 10, companhia essa integrante da Força Bilateral Cruz do Sul com o Exército do Chile.
7. Major (EA) Pablo Olmedo: Oficial Assessor de Estado Major. Suas principais funções na área foram ter sido Chefe de Pelotão na Companhia de Comunicações Satelitais, sendo um dos precursores dessa subunidade, ter sido Chefe de Companhia de Redes e Sistemas e Subcomandante do Batalhão de Comunicações 602 (com responsabilidade na infra-estrutura crítica de TIC do Exército Argentino), função que atualmente desempenha, e ter trabalhado na área de operações e desenvolvimento da Diretoria Geral de Comunicações e Informática.
8. Major (EA) Pablo Alejandro Cañete: Oficial de Estado Maior do Exército Argentino, Oficial de Estado Maior Conjunto, Especialista em Guerra Eletrônica formado na Argentina e na França, foi Chefe de Pelotão na Companhia de Comunicações Satelital e formou parte de equipe de criação da Diretoria de Defesa cibernética do Exército Argentino.

Atualmente está fazendo o Curso de Comando e Estado Maior na Alemanha.

9. Major (EA) Eugenio Olivera: Oficial Assessor de Estado Maior. Foi Comandante da Comandante da Companhia de Comunicações Satelital e atualmente é o Comandante do Primeiro Esquadrão de Comunicações e responsável da segurança cibernética da Primeira Brigada Blindada do Exército.
10. Major (EA) Christian Ariel Grogovinas: Oficial de Estado Maior do Exército Argentino, Oficial de Estado Maior Conjunto. Foi Chefe de Seção da Companhia de Comunicações Conjunta com responsabilidade na segurança informática das formações dependentes do Estado Maior Conjunto das Forças Armadas. Atualmente é o Sub Comandante do Batalhão de Operações Eletrônicas 601, desenvolvendo um projeto de experimentação da vinculação entre a cibernética e a guerra eletrônica.
11. Major (EA) Christian Gimenez: Oficial Engenheiro Militar do Exército Argentino, com mestrado na Universidade Tecnológica Nacional. Suas principais funções foram, além da sua formação técnica na área, ter sido Chefe de Companhia de Redes e Sistemas do Batalhão de Comunicações 602 (com responsabilidade na infra-estrutura crítica de TIC do Exército Argentino) e Chefe do Teleporto Satelital do Exército Argentino.
12. Major (EA – R) Héctor Ocaranza: Oficial Engenheiro Militar, com mestrado na Universidade Tecnológica Nacional e especialização em segurança informática.No âmbito militar suas principais funções na área foram no Batalhão de Comunicações 602 como Comandante da Companhia de Redes e Sistemas, tendo como responsabilidade principal na época do seu comando a migração dos sistemas nodais da Rede Digital de Sistemas de Comunicações do Exército, que é o baseamento fundamental da estrutura de TIC do Exército, com todas as problemáticas de segurança informática que isso implica. Ao passar à reserva foi contratado pela empresa ARSAT, organização com capitais públicos e privados de controle satelital de nível nacional e responsável do monitoramento e evolução da plataforma de TIC nacional. Continua trabalhando nessa empresa, na área de segurança informática, até agora.

13. Major (EA – R) Ramiro Pérez: Oficial Engenheiro Militar com especialidade em informática. Sua principal função na área de segurança informática e defesa cibernética foi ser Chefe da Divisão Informática da Contaduria Geral do Exército, responsável da informatização e segurança informática da liquidação de salários de mais de 60 mil membros do Exército Argentino, função que ocupou durante dez anos (até o ano 2017). Atualmente tem sua própria empresa de segurança informática empresarial.
14. Major (FAA) Roger Borgoñón: Oficial Engenheiro Aeronáutico, Oficial de Estado Maior Conjunto das Forças Armadas, professor universitário e especialista em telecomunicações e informática. Além das suas funções de segurança informática em plataformas aéreas (aeródromos), tem desenvolvida a teoria da anti-fragilidade que foi produto de uma tese apresentada em 2017.
15. Capitão de Fragata da (ARA) Anselmo Herrera: Oficial de Estado Maior da ARA, Oficial de Estado Maior Conjunto e especialista em Comunicações Navais. Além das funções exercidas no âmbito das comunicações navais, atualmente se desempenha Chefe de Comunicações do Comando de Comunicações e Informática Naval.
16. Capitão de Corbeta (ARA) Juan Acosta: Oficial de Estado Maior da ARA, Oficial de Estado Maior Conjunto e especialista em Comunicações Navais. Além das funções exercidas no âmbito das comunicações navais, atualmente se desempenha no staff do Comando de Comunicações e Informática Naval, com responsabilidade na segurança informática do Edifício Libertad.
17. Capitão (EA) Juan Moreira: Oficial do Sistema de Computo de Dados, Licenciado em Sistemas Informáticos, com especialidade em segurança informática e defesa cibernética. Desempenha funções no staff do Departamento Engenharia do Comando Conjunto de Defesa cibernética, realizando as atividades próprias de forênsia e resiliência cibernética.
18. Capitão (EA) Hugo Hege: Oficial do Sistema de Computo de Dados, Licenciado em Sistemas Informáticas, com especialidade em segurança informática e defesa cibernética. Desempenhou-se no staff do Departamento Informática a Diretoria Geral de Comunicações e

Informática durante 10 anos, na área de segurança informática, chegando a ser o Chefe da Divisão de Segurança Informática. Atualmente se desempenha como Oficial de Informática do Comando da Segunda Brigada Blindada.

19. Capitão (EA) Juan Funes: Oficial do Sistema de Computo de Dados, Licenciado em Sistemas Informáticas, com especialidade em segurança informática e defesa cibernética. Desempenhou-se no Batalhão de Comunicações 602 como Chefe de Pelotão Redes Informáticas e no staff do Departamento Informática a Diretoria Geral de Comunicações e Informática até a atualidade, na área de segurança informática, sendo hoje o Chefe da Divisão de Segurança Informática.
20. Tenente (EA) Marcos Francisco: Oficial do Sistema de Computo de Dados, Licenciado em Informática e especialista em Segurança Informática. Entrou ao Exército no Batalhão de Comunicações 602 no ano 2012 com uma bagagem já muito ampla na área da segurança informática no âmbito privado. Entrou como especialista na área para o desenvolvimento de plataformas de segurança informáticas do sistema de correio e administração de servidores do Exército. Produto da sua eficiência continua na área trabalhando conjuntamente com a Diretoria de Defesa cibernética do Exército Argentino e com o Departamento Informática da Diretoria de Comunicações e Informática do Exército.
21. Gabriel Stanley: Especialista em informática com bases sólidas dadas pela sua experiência nas áreas de programação, de SAP (Sistema Integrado de Gestão Empresarial) e segurança informática. Fundador da sua própria empresa de assessoria informática baseada principalmente em gerar estruturas informáticas a pedido do cliente, garantindo à empresa eficiência, segurança da sua informação e rapidez.
22. Capitão (EA) Baltazar Waterloo: Engenheiro em Sistemas, se desempenha na atualidade como Chefe da Seção de Operações Conjuntas no Comando Conjunto de Ciberdefesa da República Argentina, função que desempenha faz 4 anos.
23. Tenente Coronel (EA) Marciel Rene Dasso: Oficial da Arma de Comunicações, Licenciado em Estratégia e Organização. Atualmente se desempenha como Chefe de Divisão Educação e Doutrina do Comando

Conjunto de Ciberdefesa. Pesquisador na área de Ciberdefesa. Atualmente Mestrando em Ciberdefesa e Cibersegurança na Universidade de Buenos Aires.

24. Major Eduardo Malvacio: Oficial Engenheiro Militar em Informática. Atualmente desempenha funções na Diretoria de Ciberdefesa do Exército Argentino. Possui 6 anos de experiência na área.

ANGOLA:

25. Daniel Geto: Estudante de Engenharia em Informática na Angola, na área de redes e telecomunicações. Pesquisador na área de ciberdefesa e cibersegurança. Possui 3 anos de experiência na área.
26. Domingos Balundo: Engenheiro. Desempenha funções na organização ITEL da Angola. Possui 5 anos de experiência na área.

BRASIL:

27. Coronel João Carneiro: Oficial do Quadro de Estado Maior da Ativa, especialista em Defesa cibernética, atualmente destinado nos Estados Unidos de América na área de pesquisa e desenvolvimento de cibernética. É professor no Colégio Interamericano de Defesa desse país, referente no Brasil na área, e tem uma experiência de mais de 30 anos na área das TIC.
28. Major Flavio Costa Regueira: Oficial do Quadro de Estado Maior da Ativa, especialista em Defesa cibernética, atualmente destinado no CDCIBER, e possui uma experiência de 5 anos na área da cibernética.
29. Professor Doutor Leonardo Perin Vichi: Doutorando do IMM e pesquisador na área de Defesa cibernética. Membro do Observatório Militar da Praia Vermelha. Atualmente se desempenha como professor na Escola de Guerra Naval e é um ativo pesquisador e conferencista na área de ciberdefesa.
30. Breno Pauli Medeiros: Doutorando do IMM e pesquisador na área de Defesa cibernética. Membro do Observatório Militar da Praia Vermelha. Atualmente se desempenha como adjunto acadêmico e pesquisador na área da ciberdefesa.
31. Marcelo Malagutti: Doutorando do IMM. Pesquisador na área de Defesa cibernética. Membro do Observatório Militar da Praia Vermelha. Graduado

em Ciências da Computação, com mais de 25 anos de experiência no desenvolvimento de sistemas de automatização bancária. Desde que cursou a ESG no Brasil em 2010 virou pesquisador na área de ciberdefesa e cibersegurança, tendo feito o mestrado no Kings College London com dissertação sobre ciber- dissuasão para nações com uma cultura não agressiva, tema que encontra-se aprofundando no doutorado.

32. André Nery: Licenciado em Física. Mestrando do IMM e pesquisador na área de Defesa cibernética. Atualmente se desempenha na empresa Ancine como analista de infraestruturas de segurança da informação. Possui experiência nas áreas de segurança cibernética, redes de computação e infraestruturas de TI.

COLÔMBIA:

33. Tenente Coronel Fernando Rocero: Especialista em Cibernética e atualmente destinado no Comando Conjunto de Defesa cibernética da Colômbia. Possui uma experiência na área de 5 anos.
34. Capitão Carlos Medina: Especialista em Cibernética e atualmente destinado no Comando Conjunto de Defesa cibernética da Colômbia. Possui uma experiência na área de 5 anos.

CHILE:

35. Jorge Antonio Revillot Garreton: Engenheiro, membro da empresa SwissCom, sendo na atualidade Chefe de Divisão na área de Ciência e Tecnologia, atendendo a problemática da cibersegurança e segurança informática da sua organização. Tem 5 anos de experiência na área. É pesquisador na área de cibersegurança.

CHINA:

36. Coronel Shang Jing: Coronel do Exército Chinês, integrante da Academia de Comando e Estado Maior do Exército Chinês. É professora associada. Dedicação ao ensino e pesquisa na teoria sobre operações cibernéticas e eletromagnéticas. Trabalhou como oficial encarregada na Seção de Informatização de um Corpo de Exército da China.

EL SALVADOR:

37. Capitão Leonel Maye: Licenciado em informática. Desempenha-se na atualidade no Ministério da Defesa do seu país, na função de Chefe de Desenvolvimento na área de Defesa Cibernética (S-SLDC). Tem uma experiência de 8 anos nessa área.

EQUADOR:

38. Engenheiro Romel Aldás: Engenheiro em Informática atualmente cumprindo funções na organização Cimse, sendo sua especialidade a simulação. Com 12 anos de experiência na área, é pesquisador e operador na área da ciberdefesa.
39. Tecnólogo Alex Narváez: Tecnólogo em análise de sistemas se desempenha como especialista técnico no Comando Conjunto de Ciberdefesa do Equador.
40. Engenheiro Freddy Laica: Engenheiro em informática. Atualmente desempenha funções como técnicas em segurança informático no Comando Conjunto de Cibernética do Equador. Possui uma experiência de 7 anos na área.
41. Sargento Segundo Juan Montalvo: Técnico em simulação. Atualmente se desempenha como técnico no Centro de Simulação do Exército Equatoriano. Tem uma experiência de 4 anos na área.
42. Tenente Coronel Santiago Narvaez: Atualmente se desempenha como Chefe de Operações do Comando de Ciberdefesa do Exército Equatoriano.
43. Engenheiro Marco Ojeda: Engenheiro e Mestre na área de sistemas informáticos. Atualmente se desempenha como Diretor de Departamento na organização ESPE do Exército Equatoriano.
44. Cabo Alex Ivan Caiza Plasencia: Técnico em Simulação. Atualmente se desempenha na área de manutenção informática. Pertence à organização ESPE do Exército Equatoriano.

ESPANHA:

45. Professor Doutor Alejandro Raúl Corletti Estrada: Doutor em Engenharia, Engenheiro Militar, mestre em Informática, MBA, professor universitário, experto em Defesa cibernética. Como militar da ativa do Exército Argentino foi o criador da Rede De Integração de Sistemas do Exército que na década dos 90 era uma inovação sem precedentes. Começou trabalhar

nesse período para a empresa Telefônica de Argentina, continuando até agora, mas numa posição de relevância como consultor e assessor na empresa global do Grupo Telefônica, na área de Direção Corporativa de Auditorias em Redes e Sistemas. Diretor da empresa DarFe Learning Consulting S.L. na Espanha. É conferencista internacional, assessor em matéria de Defesa cibernética de organismos nacionais e internacionais, pesquisador na área de cibernética e têm inúmeras publicações (livros e artigos) relacionadas com a matéria.

46. Comandante Alberto Díaz: Oficial del Ejército del Aire da Espanha com responsabilidade na área de ciberdefesa. Atualmente se desempenha como Chefe de Divisão no Centro de Operações de Ciberdefesa. Tem 5 anos de experiência na área.
47. Tenente Coronel Mariano Fortiz: Oficial del Ejército de Tierra da Espanha com responsabilidade na área de ciberdefesa. Atualmente se desempenha como Chefe de Divisão no Comando Conjunto de Ciberdefesa. Tem 5 anos de experiência na área.
48. Embaixadora Alicia Moral: Ex Embaixadora na missão especial de cibersegurança da Espanha ante a OTAN. Atualmente se encontra trabalhando na Escola de Guerra da Espanha, que é de nível conjunto. Possui 6 anos de experiência na área.

ESTADOS UNIDOS DE AMÉRICA:

49. Engenheiro Alex Govornov: Engenheiro da área de Informática, atualmente trabalhando para a empresa norte-americana ATT. Ocupa a função de Head of Department e possui uma experiência na área de 5 anos.
50. Major Rose Abido: Oficial do Exército dos Estados Unidos da América especializada em ciberdefesa. Atualmente é aluna do Army War College. Possui uma experiência na área de 6 anos.
51. Major Peter Sean: Oficial do Exército dos Estados Unidos da América especializado em ciberdefesa. Atualmente encontra-se desempenhando a função de Liaison Officer in the Cyber Defense Command of Germany. Possui 7 anos de experiência na área e participou dos últimos eventos oferecidos pelo Centro de Excelência Cooperativo de Ciberdefesa na Estônia

52. Engenheiro Eric Sutton: Engenheiro na área de informática. Atualmente desempenha funções de Senior Patent Counsel at Oracle Corporation. Possui 6 anos de experiência na área.

GUATEMALA:

53. Mayor Fabricio Verganza: Oficial do Exército de Guatemala que se desempenha como Chefe de Divisão no Comando de Ciberdefesa. Possui 5 anos de experiência na área.

MÉXICO:

54. Engenheiro Rodrigo Ayala: Engenheiro em Informática do México. Atualmente se desempenha na Equipe de Resposta a Incidentes, no marco da organização SEDENA. Possui 10 anos de experiência na área.
55. Tenente Coronel Víctor Hugo Sánchez Huerta: Engenheiro em Informática. Atualmente desempenha funções na Secretaria da Defesa do México. É Chefe de Coordenação na Chefia do EMDN.

PARAGUAI:

56. Major José Ojeda: Oficial da Arma de Comunicações do Exército do Paraguai. Desempenhou funções da área de Ciberdefesa do Exército paraguaio. Atualmente se desempenha como Observador Militar das Nações Unidas.

PERU:

57. Coronel Ivan Loaiza Abregú: Oficial Superior do Serviço de Comunicações do Exército Peruano. Atualmente se desempenha como Diretor de Telemática e Estatística do Exército. Possui 5 anos de experiência na área.

URUGUAI:

58. Major Rubén Brum: Licenciado em Ciências Militares, Oficial de Estado Maior, Oficial de Inteligência e Especialista em Inteligência Estratégica. Oficial da Arma de Comunicações, mas a partir do ano 2007 se especializou na área de inteligência. Pesquisador na área de Ciberdefesa. Atualmente encontra-se cursando a Licenciatura em Ciberdefesa.